The National Electronic Commerce Coordinating Council

Identity Management

A White Paper

Presented at the NECCC Annual Conference, December 4-6, 2002, New York, NY

National Electronic Commerce Coordinating Council

In 1997, as the use of the Internet was increasing at a stunning rate, a group of public and private professionals — government executives and information technology practitioners — met in San Antonio, Texas to discuss their common issues, problems and ideas. This first meeting was productive. Participants learned from each other. They felt that continuing to meet as a group would help them meet the challenges and opportunities posed by the rush of engulfing information technologies. This founding group formed the National Electronic Commerce Coordinating Council (NECCC), which has continued to meet regularly.

Today, NECCC serves as an alliance of government organizations dedicated to promoting electronic government through the exploration of emerging issues and best practices. Alliance partners are the National Association of State Auditors, Comptrollers and Treasurers; the National Association of Secretaries of State NASS; and the National Institute of Governmental Purchasing.

NECCC also works in partnership with these affiliate organizations: the Information Technology Association of America; National Automated Clearing House Association; National Association of Government Archives and Records Administrators; and National Association of State Treasurers

Contact Information

The National Electronic Commerce Coordinating Council
2401 Regency Road, Suite 302
Lexington, KY 40503
P: (859) 276-1147
F: (859) 278-0507
www.ec3.org

2002 NECCC Executive Board

Signatory Members

Chair, *J. Kenneth Blackwell*, NASS, Secretary of State, Ohio
Vice Chair, *Ralph Campbell, Jr.*, NASACT, State Auditor, North Carolina
Secretary/Treasurer, *Mary Kiffmeyer*, NASS, Secretary of State, Minnesota

Steve Adams, NASACT, State Treasurer, Tennessee
David Dise, NIGP, Procurement Manager, Fairfax County Water Authority, Virginia
Rick Grimm, NIGP, NIGP Chief Executive Officer, Virginia
Stephen Gordon, NIGP, Purchasing Agent, Metropolitan Govt. of Nashville/Davidson
County, Tennessee
Elaine Marshall, NASS, Secretary of State, North Carolina
Robert Childree, NASACT, State Comptroller, Alabama

Affiliate Members

P.K. Agarwal, ITAA, CIO and Executive Vice President, National Information Consortium
William Kilmartin, NACHA, Vice President, Accenture
Jack Markell, NAST, State Treasurer, Delaware
Amelia Winstead, NAGARA, State and Local Government Services Manager, Office of the Secretary of State, Georgia

Ex-Officio Members

Carolyn Purcell, CIO, Department of Information Resources, Texas
Basil Nikas, CEO, iNetPurchasing
J.D. Williams, Director, State and Local Government, PeopleSoft, USA, Inc.

At-Large Members

Avi Duvdevani, CIO/Deputy General Manager, New York
Daniel Greenwood, Director, MIT E-Commerce Architecture Program, Massachusetts Institute of Technology
David Lewis, Retired Director and CIO, Massachusetts
Jay Maxwell, Senior Vice President, AAMVA
Eric Reeves, State Senator, North Carolina
David Temoshok, PKI Program Manager, Government Services Administration
Costis Toregas, CEO, Public Technology, Inc.
Susan Hogg, Chief, Statewide e-Government Initiatives Office

Members of the Identity Management Work Group

Leadership
Daniel Greenwood, Director, E-Commerce Architecture Program, MIT
Mary Kiffmeyer, Secretary of State, Minnesota

Drafting Team
Dan Combs, Director of Digital Government, Iowa
Ed Fraga, Vice President, Public Sector Practice, Gartner Consulting
Daniel Greenwood, Director, E-Commerce Architecture Program, MIT

Contributors to the Paper
Paula Arcioni, PKI & Directory Services Manager, Office of Information Technology, New Jersey
Dan Combs, Director of Digital Government, Iowa
Rich Dymalski, Principal IT Consultant, Office of the CIO, Maricopa Co., Arizona
Ed Fraga, Vice President, Public Sector Practice, Gartner Consulting
Daniel Greenwood, Director, E-Commerce Architecture Program, MIT
Linda Hamel, General Counsel, ITD, Commonwealth of Massachusetts
John Messing, Consultant, Law-on-Line, Inc.
Jack Radzikowski, Identix
Helena Sims, Senior Director, NACHA

Other Members of the Work Group
John Aveni, Associate Counsel, Strategic Policies, Acquisitions and e-Commerce, Office for Technology, New York
Susan Cromwell, Chair, State Land Information Board, Arkansas
Michele G. Foley, DP Fiscal Systems Auditor II, Office of the State Comptroller, New York
Barry Goleman, Vice President, American Management Systems
Peter Goolsby, Analyst, Department of the Secretary of State, North Carolina
Maureen Haggerty, Information Technology Manager, Administrative Office of the Courts, Arizona
Kenny Holmes, Systems Engineer, Entrust
Gary Johnson, Technology Planning Specialist, Office of Information Technology, Arkansas
Jerry Johnson, Senior Policy Analyst, Department of Information Resources, Texas
Michael Kerr, Senior Program Manager, Enterprise Solutions Division, ITAA
Alan Kowlowitz, E-Commerce/E-Government, Office for Technology, New York
Kym Patterson, Security Policy Coordinator, State Security Office, Arkansas
Leslie Reynolds, Executive Director, NASS
Doug Robinson, Executive Director, Governor's Office for Technology, Office of Policy and Customer Relations, Kentucky

Russ Savage, Electronic Transactions Liaison, Office of the Secretary of State,

Arizona
Eric Seabrook, General Counsel, Office of the Secretary of State, Ohio
Tom Stack, Maximus
David Temoshok, Director, Identity Policy/Management, Office of Governmentwide Policy, GSA
Harsh Verma, Senior IT Consultant, California

This page left blank intentionally.

Table of Contents

1. INTRODUCTION……9

   1.1 Vision of Identity Management……10

   1.2 Scope……..10
   1.2.1 Purpose of this White Paper

   1.3 Intended Audiences……..11
   1.3.1 The Target Audience
   1.3.2 The Stakeholder Audience

2. CURRENT ENVIRONMENT: IDENTITY MANAGEMENT TODAY……11

   2.1 Private Sector Activity……12
   2.1.1 Private Sector Organization Aims for Identity Management
   2.1.2 Microsoft Passport
   2.1.3 Liberty Alliance

   2.2 Public and Private Systems: Similarities and Differences in Identity Management Drivers and Inhibitors……14

   2.2.1 e-Tailing and the Drive for “Usernames”
   2.2.2 e-Government and the Drive Toward Integration
   2.2.3 Governmental, Law Enforcement and Intelligence Interest in Single Identity
   2.2.4 Fair Information Practices: Citizens Managing Their Own Identity

   2.3 Public Sector Legislative Activity……17
   2.3.1 Civil and Commercial Identity-Related Federal Legislation
   2.3.2 Counter-Terrorism and Security-Related Federal Legislation
   2.3.2.1 The Aviation and Transportation Security Act
   2.3.2.2 The USA Patriot Act
   2.3.2.3 The Port and Maritime Security Act
   2.3.2.4 Enhanced Border Security and Visa Entry Reform Act
   2.3.3 State Government Legislation

   2.4 Public Sector Executive Activity……..20
   2.4.1 Federal Executive
   2.4.2 State Executive
   2.4.2.1 State of Massachusetts
   2.4.2.2 State of Iowa

3. APPROACHES……23

   3.1 Single Federal National System……..24

   3.2 State Federated System……24

   3.3 Systemic Uniformity: Part of the “Management” in Identity Management…….26

4. ANALYSIS……27

   4.1 Identity Systems Are Not Homogenous Because Identity Is Not Homogenous…27

4.2 Factors to Consider……27
4.2.1 The Context in Which Identity Arises
4.2.1.1 Central Authority
4.2.1.2 Individual Citizen
4.2.1.3 Autonomous Group
4.2.2 Policy and Political Synthesis
4.2.3 Drill-Down: Central Authority E-Government and Citizen Identity Perspective
4.2.4 The Nature of Transaction
4.2.5 Regulation of Private Parties: Federal ESIGN Issues
4.2.6 Risk Management
4.2.6.1 MIT eCap Risk Management Method for E-Business and E-Government
4.2.7 Latitude & Attitude: Differences in Risk Perception by Region and Jurisdiction

4.3 Identity Management Principles……..39

5. CONCLUSION……41

Appendix A – Glossary of Terms……43

Appendix B – The Starting Point: Common Practice and Common Law……..47

Appendix C – Commercial Investment at U.S. Ports of Entry……51

Appendix D – California Privacy-Related Laws……55

Appendix E – Fair Information Practice Principles……61

Identity Management

1. Introduction

For leaders in the public sector, the emerging debate over identity management and the selections of technology to authenticate citizens and business will be among the most important of all matters to shape the coming information age. Indeed, as with so many issues central to government leadership in the information age, the key ideas are as old – or older – than the country itself. So it is with the recently invigorated debate over identity management. The competing policy interests range from protecting citizen freedoms, privacy and other prerogatives on one end of the scale to ensuring law, order, national security, and institutional efficiencies on the other end. Indeed, the philosophical and political implications of choosing various proposed solutions cut to the core of the relationship between government and citizen – is creation and use of a person's identity flatly subject to central decree or must it be based upon consent of the governed? The current system of identity in the United States is, at best, a patchwork of different – sometimes inconsistent – processes, practices and rules of law.

Key Questions for Policy Makers

Among the key questions of the day: is it desirable to require a single national ID for all citizens? Whether or not it is desirable, is it necessary in order to preserve order and national security? Is it necessary to avoid such an ID scheme in order to preserve civil liberties and prevent inevitable misuse and abuse by centralized unaccountable authorities? Are there other creative ways to accomplish the legitimate business, law enforcement, intelligence and civilian government objectives that drive the need for more efficient identity management? What is the proper balance between the competing public policy interests at hand? How does the selection of technical architectures carry within it implied or explicit public policy choices, whether intended or not, by the proper decision makers?

Background

Identity management of citizens, organizations and other public institutions has been a core function of governments for millennia. Taken as a historical reference, the Bible story of Joseph and Mary traveling to the town of Bethlehem to register for the census over 2,000 years ago indicates that there was already at that time an established role for government in the identification of its citizens. The issues involved in creating, using, changing and ending an identity involve technical, procedural, legal and policy dimensions. The advent of the information age has raised many of these issues anew. Current information management capabilities provide tremendous leverage in accessing, processing, manipulating

and stealing information. This raises questions of privacy, security and fair information practices on the one hand, to be balanced against convenience of e-government service delivery, the need to identify and apprehend terrorists and fraud artists, and the need to interoperate across government and private systems on the other hand.

As states continue to integrate information systems to accumulate the benefits of digital government for citizens and business users such as portals or common access points for multiple services and single login or sign-on functions per session, the need for some form of identity management at the state enterprise level will increase. Beyond internal uses, given that most "core" identification of citizens is customarily done at the local or state levels through devices such as birth certificates, death certificates, driving licenses and so forth, it is clear that policy makers at the state and local levels will become increasingly important to the debate over the future of identity in the United States.

State governments have always been in the identity "business" whether by choice or default. Due to the wide-ranging effects of weak or ineffective identity services, if states are to remain involved in this service there is a responsibility to citizens to perform that service well. If states should decide to abdicate that responsibility, the private sector or other levels of government will of necessity try to fill the void. That would likely result in a lower quality, more expensive solution. The decision regarding the degree of state involvement in identity issues should be based on good information and well-informed reasoning.

1.1 Vision of Identity Management

The vision for state Identity Management is a system of technologies, business practices, laws and policies that would:

- Support common identity needs of governmental and private transactions.
- Reduce the costs of government and/or enhance government service quality.
- Safeguard the health and safety of the public.
- Preserve or improve individual privacy, name and identity related liberties, and the security of identity information.

1.2 Scope

1.2.1 Purpose of This White Paper

The purpose of this identity management white paper is to:

1. Educate government and non-government decision-makers about identity management.
2. Identify approaches to achieving identity management.

3. Suggest an appropriate role for state governments in identity management.
4. Provide a contribution to, and stimulus for, further dialogue regarding identity management and the role of government in it.

1.3 Intended Audiences

1.3.1 The Target Audience

The target audience of this identity management white paper (the audience to which this paper is addressed) is:

1. State elected officials especially governors, legislators, and secretaries of state.
2. State appointed officials, especially chief information officers, IT directors and their staffs and government business units involved in the creation and use of identities.

1.3.2 The Stakeholder Audience

The stakeholder audience of this identity management white paper (the audience that could be expected to have an interest in, and to read, this paper) is:

1. Local, state and federal elected officials, especially those involved in the creation and use of identities.
2. Local, state and federal appointed officials, especially those involved in the creation and use of identities.
3. Governments of other countries.
4. Government and non-government associations, especially those concerned with consumer advocacy, information systems and the role of government in identity management.
5. Vendors, especially those involved in the development and sale of identity management, privacy and security products and services.
6. Active citizens and advocacy organizations interested in privacy, fair information practices and information age public policy.

2. Current Environment: Identity Management Today

Consideration of policy setting and selection of technical systems for use within and by state governments in the area of identity management must be sensitive to the current legal and business environments. This area of activity remains unsettled, but there are certain factors and trends that will be relevant to any decision-maker at this time. The use and evolution of solutions for identity management from the private sector are an important part of the national picture. States must take into account private sector offerings as a critical input to the

range of possible alternatives. Collaboration between public and private institutions will be key to addressing this issue set. The following is a survey of the relevant issues and "facts on the ground" in the public and private sectors.

2.1 Private Sector Activity

2.1.1 Private Sector Organization Aims for Identity Management

The goals of the private sector in creating and using identity management systems have similarities and differences from those of the public sector. One key similarity is that both the public and private sectors wish to enable a system that will allow an end user (whether an individual or organization) to enjoy the convenience of "single sign-on."[1] Both sectors also desire to enhance so-called Customer Relationship Management (CRM) methods and increase opportunities to spot fraud against their systems.

The private sector has additional needs to enable faster reaction to a changing business environment. For example, mergers, reorganizations, departmental moves and other organizational changes all carry with them user identity management consequences. The public sector shares this need in some part, but to a lesser degree and in some cases (as when a merger occurs) in a qualitatively different way.

Identity management in the private sector can also implicate basic business strategy, marketing and industry configurations. For example, a company may wish to leverage its superior market position to further "lock in" customers by creating a proprietary single sign-on system to intermediate business relationships between its customers and other private companies. Another example would be when companies of roughly comparable market power agree among themselves to federate by sharing customer authentication system processes so users can easily buy from any member of the club. This could create a competitive advantage against companies outside the federation. The profit motive drives the private sector results in these and many other examples of different goals and requirements for identity management systems than those of the public sector.

However, it remains to be seen whether there are systems and processes that can be used across the public and private sectors. While current architectures appear to be primarily or exclusively suitable in one or the other sector, it is clear that ultimately there will be a sufficient demand for cross-sector interoperability that common-denominator solutions will be required.

The following list illustrates some of the common drivers in the private sector toward identity management solutions:

[1] In this context, single-sign-on refers to the convenient of identifying and authenticating oneself only once for a series of transactions instead of repeatedly for each transaction.

- *Organizational Efficiency*. Enable transactions and person-to-person communication.
- *Competitive Advantage*. Capturing new or larger shares of markets and enhancing company position against competitors.
- *Security*. Enable authorized access and prevent unauthorized access to information and services
- *Speed of Reaction to Change*. Mergers, reorganizations, departmental moves.
- *Fraud Prevention*. Hard to quantify, but can clearly provide major savings.
- *Consistent Treatment of the Individual*. "End-to-end" management of employees, "single view of the customer," "joined-up government."
- *Integrated Information Infrastructure*. Enable move away from "information silos" and "IT-processing chimneys."

2.1.2 Microsoft Passport

According to the Microsoft Passport Web site, a consumer can "use one name and password to sign in to all .NET Passport-participating sites and services. Store personal information in your .NET Passport profile and, if you choose, automatically share that information when you sign in so that participating sites can provide you with personalized services."[2] In essence, this is a centralized corporate identity system run by Microsoft and used by Microsoft customers and Microsoft business partners or other affiliates. To be a customer requires only agreement to the terms and conditions set forth by Microsoft, and participation is at this time free of charge to the end user.

2.1.3 Liberty Alliance

- Liberty Alliance is a consortium of vendors, which does not include Microsoft. Liberty Alliance is working on the development, deployment and evolution of an open, interoperable standard for network identity where privacy, security and trust are maintained.
- The primary goals of the Liberty Alliance Project are:
  - To allow individual consumers and businesses to maintain personal information securely.
  - To provide a universal open standard for single sign-on with decentralized authentication and open authorization from multiple providers.
  - To provide an open standard for network identity spanning all network devices.

[2] http://www.passport.net/Consumer/default.asp?lc=1033 last visited on 10/9/02

2.2 Public and Private Systems: Similarities and Differences in Identity Management Drivers and Inhibitors

2.2.1 e-Tailing and the Drive for "Usernames"

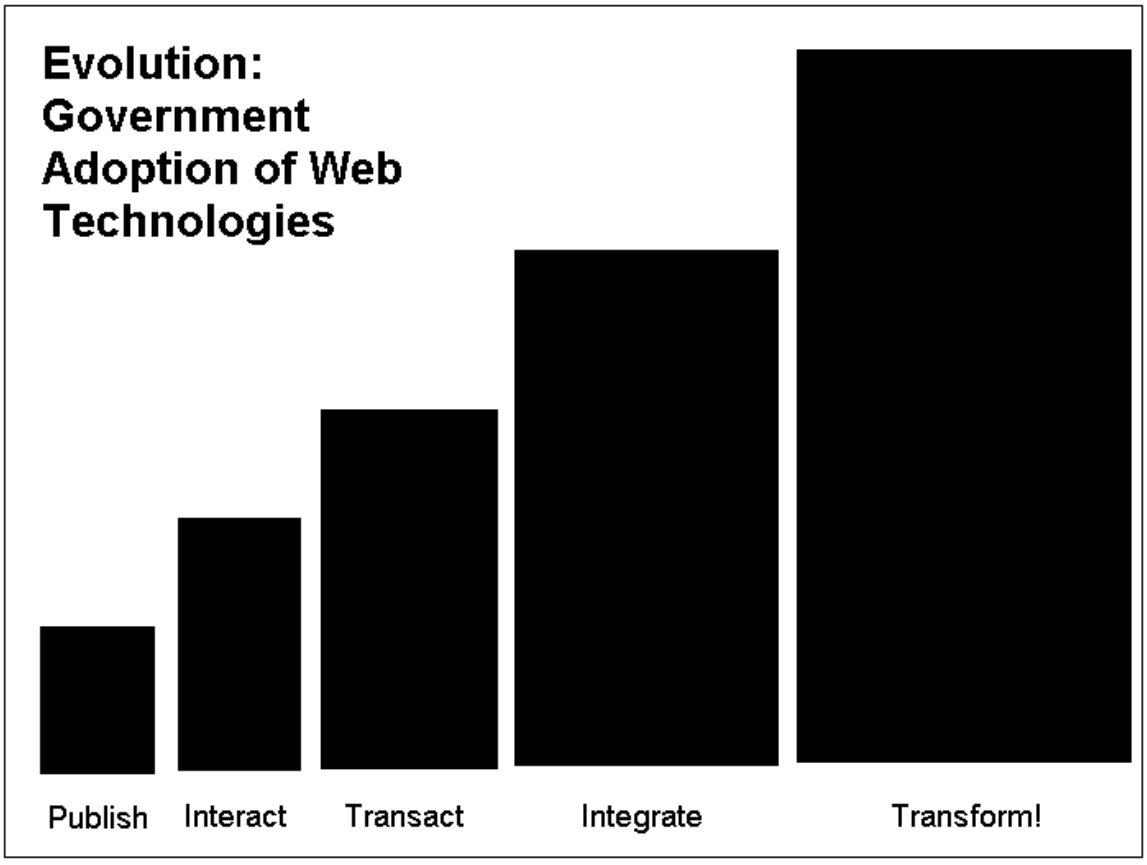
When a traditional transaction is accomplished electronically, it is quite likely that the individual will be required to complete a new user registration process, agree to lengthy terms and conditions, and use a form of payment (typically credit card) that provides a high degree of certainty as to the user's identity. Leaving aside the related policy issues of undesired direct marketing and the process of consenting to have one's personal information shared among business affiliates, it is important to note that the business transaction environment for personal identity is potentially dramatically different when conducted online versus offline. The reasons for these differences, in the retail environment at least, are fairly clear: immediate transactions require immediate electronic payment options; the opportunities for fraud and misuse of automated systems are potentially different in terms of scale and velocity (e.g. hackers can potentially conduct many fraudulent transactions in a short time); and a perceived business value is assigned to so-called CRM, whereby a business Web site operator can track the activities and communications with a customer over time to provide higher levels of service and better manage market expectations. But these modern methods of identifying and continually authenticating customers throughout an online relationship have consequences far beyond the initial business drivers.

2.2.2 e-Government and the Drive Toward Integration

The same types of transitions are occurring (albeit more slowly) in the public sector. State government portals are increasingly offering or requiring a user ID for citizens or businesses to access parts of the public sector Web presence. The specific drivers in the public sector are better understood with reference to following diagram illustrating the five stages of Web-enabled evolution in the public sector. The usual first step in adopting a Web presence for a government agency is to publish a static Web site. A static site usually displays straight text about such things as the agency mission, hours of operation and address and other helpful information, and is like a brochure or infomercial in that it is delivered in a "one size fits all" and "one to many" broadcast style. The next stage of evolution in the adoption of Web technologies will often involve the incorporation of interactivity into the Web site. For example, a user might be able to input a zip code to get a dynamically generated screen showing all the widget registries in a specific area. This technology involves use of a database and a means of generating new screens of information on the user's Web browser according to the information queried or input by the user.

The next stage of development is to turn some of those interactions into transactions. In other words, allowing users to conduct a formal or business type of transaction via the Web with the agency. Tax filings, license renewals and

grant applications area examples of these types of transactions. In this context, the term transaction does not necessarily have to involve the transfer of money – though it typically does. Filling out an official form or making official statements should be considered a transaction because such conduct changes the rights and responsibilities of the parties in important ways and can lead to serious consequences. After enabling a number of transactions, one or more agencies will feel pressure to begin to make it easy for the user and for the back-office personnel and systems to start to integrate some of the related transactions. For example, it is common for a business to have to file forms with many state (and other) government departments when hiring a new employee. Rather than making the business start fresh on each agency Web site, and fill out much of the same information multiple times, integrating the process into a single interface and transaction is more convenient, faster, and less expensive. Theoretically, once enough transactions and interactions have been integrated from the point of view of the citizen or business, then in a very real sense, the government as an entity is transformed. This is certainly true in the eyes of the persons dealing with government. But it will also be true in that these sorts of front-end integrations will force back-end government changes like interoperability of systems, business processes, and organizational structure that would otherwise not occur. The dream is that this will constitute a transformation of government from a rigid, bureaucratic, inward-looking industrial style organization to a more agile, responsive, accountable and transparent customer-centered organization.



2.2.3 Governmental, Law Enforcement and Intelligence Interest in Single Identity

One of the prerequisites for integrated transactions is integrated ways of dealing with the identity and authentication of a user who conducts the linked transactions. In this way, the drive toward e-government has become one of the drivers for better identity management and authentication of customers. Tying the various usernames and numbers of customers from different agency systems together becomes one of the keys to achieving integration.

Other public sector drivers toward identity management include a desire to better detect, track and catch terrorists – especially in the post attack period in which we now exist. Federal legislation has been enacted to tighten identity document requirements for certain members of the transportation sector. Civilian air travel and border crossing has all become the subject of greater scrutiny of identity. In addition, basic law enforcement techniques are also being enhanced by the availability of user authentication data. Combating identity fraud may become one of the biggest drivers for better citizen identity management systems in the future. Ironically, more tightly linked identity systems can also serve as a large problem for those citizens that fall subject to identity theft, or worse – fall victim to mistakes or abuse by those who control the systems. This unintended consequence has not been sufficiently considered in the major schemes put forward to date.

Criminals and fraud artists, however, use computers in ways that far exceed simple on-line fraud. Being able to piece back together trails of digital activity and attribute it to a defendant is an invaluable “arrow” in the “quiver” available for crime fighting. The basic concept is that getting the bad guys is easier when all the different identities they use to evade detection can be linked back to them.

2.2.4 Fair Information Practices: Citizens Managing Their Own Identity

Interestingly, another driver behind the concept of “identity management” comes from people themselves, and those advocates who support the right of people to protect their privacy and other personal prerogatives. In a sense, citizens are assured better management of their own identity and identity information by each statute or regulation that requires holders of personally identifiable information to be responsive to the wishes of the subject of the data. For example, the privacy rights afforded consumers in the financial sector by the federal Gramm-Leach Bliley Act can be seen as enhancing an individual’s ability to better manage an identity and use identity information. So-called fair information practices, like assuring the right of people to prevent the sharing of their identity information with third parties without their prior, explicit consent, is a core principle of citizen-centered identity management. These types of policy imperatives animate much state, federal and European law. For more information on this legal and policy area, see Appendix E and to a lesser extend Appendix D.

2.3 Public Sector Legislative Activity

2.3.1 Civil and Commercial Identity-Related Federal Legislation

There is a long and rich body of law and regulation affecting identity. The rules governing use, disclosure and protections of the social security number are a good example. For instance, under the Privacy Act of 1974, all government agencies – federal, state and local – which request social security numbers are required to provide a disclosure statement on the form. That statement tells people if they are required to provide their social security number or if it is optional, how the SSN will be used and what will happen if they refuse to provide it. Since 1990, any SSN given to a government agency cannot become part of a public record (see 5 USC 552a, note). The U.S. Office of Management and Budget, Office of Information and Regulatory Affairs (OIRA) provides guidance and oversight regarding the Privacy Act of 1974. The text of the Privacy Act can be found at the Web site www.usdoj.gov/foia/privstat.htm.

Courts have held that social security numbers fall within the scope of personally identifiable information that is restricted from disclosure by schools that receive federal funding under the Family Educational Rights and Privacy Act (FERPA, also known as the "Buckley Amendment," enacted in 1974, 20 USC 1232g). With some exceptions, this federal law requires explicit and written consent for the release of personally identifiable information. (See www.cpsr.org/cpsr/privacy/ssn/ferpa.buckley.html.)

Beyond restrictions on the use of SSN's, there are federal criminal laws prohibiting use of the password of another (Computer Fraud and Abuse Act, etc); restrictions against cross-matching of different federal databases to triangulate identity information; and federal laws or regulations governing the creation, use, sharing and deletion of personally identifiable information or electronic signatures. The following statutes are the most commonly cited as forming the basis of U.S. federal privacy statutes:

☐Children's Online Privacy Protection Act (COPPA) - 15 U.S. Code 6501 et seq. The act's goal is to place parents in control over what information is collected from their children online. With limited exceptions, the related FTC rule requires operators of commercial Web sites and online services to provide notice and get parent's consent before collecting personal information from children under 13.

☐Driver's Privacy Protection Act of 1994 - 18 U.S. Code 2721 et seq. This law puts limits on disclosures of personal information in records maintained by departments of motor vehicles.

☐Fair Credit Reporting Act (FCRA) - 15 USC 1681-1681u

This federal law is designed to promote accuracy, fairness, and privacy of information in the files of every "consumer reporting agency," the credit bureaus that gather and sell information about consumers to creditors, employers, landlords and other businesses.

www.ftc.gov/bcp/conline/edcams/fcra/index.html

☐Family Educational Rights and Privacy Act of 1974 (FERPA) - 20 U.S. Code 1232g This law puts limits on disclosure of educational records maintained by agencies and institutions that receive federal funding.

☐Federal Identity Theft Assumption and Deterrence Act of 1998 - 18 USC 1028 The act makes it a federal crime to use another's identity to commit an activity that violates federal law or that is a felony under state or local law. Violations are investigated by federal agencies including the Secret Service, the FBI and the Postal Inspection Service and prosecuted by the U.S. Department of Justice.

www4.law.cornell.edu/uscode/18/1028.html

☐Federal Privacy Act of 1974 - 5 U.S. Code 552a This law applies to the records of federal government executive and regulatory agencies. It requires such agencies to apply basic fair information practices to records containing the personal information of most individuals.

☐Financial Services Modernization Act, Gramm-Leach-Bliley (GLB), Privacy Rule - 15 USC 6801-6827 The 1999 federal law permits the consolidation of financial services companies and requires financial institutions to issue privacy notices to their customers, giving them the opportunity to opt-out of some sharing of personally identifiable financial information with outside companies.

www.ftc.gov/privacy/glbact/index.html

☐Health Information Portability and Accountability Act of 1996 (HIPAA), Standards for Privacy of Individually Identifiable Health Information, Final Rule - 45 CFR Parts 160 and 164 HIPAA includes provisions designed to save money for health care businesses by encouraging electronic transactions and also regulations to protect the security and confidentiality of patient information. The privacy rule took effect on April 14, 2001, with most covered entities (health plans, health care clearinghouse and health care providers who conduct certain financial and administrative transactions electronically) having until April 2003 to comply. http://aspe.hhs.gov/admnsimp/bannerps.htm#privacy

☐Telephone Consumer Protection Act (TCPA) - 47 U.S. Code 227 This law puts restrictions on telemarketing calls and on the use of autodialers, prerecorded messages, and fax machines to send unsolicited advertisements.

2.3.2 Counter-Terror and Security-Related Federal Legislation

One common thread across post 9/11 transportation-related legislation is the requirement for verification of the identity of individuals at security-sensitive, access control points.

2.3.2.1 The Aviation and Transportation Security Act

The Aviation and Transportation Security Act requires this for airline and airport workers.

2.3.2.2 The USA Patriot Act

The USA Patriot Act requires this for hazardous material truck drivers.

2.3.2.3 The Port and Maritime Security Act

The Port and Maritime Security Act (awaiting full House action) requires this for port workers and seafarers.

These commercial workers must undergo fingerprint-based criminal history background checks and, over time, possess smart card badges tied to the bearer via biometric reference.

2.3.2.4 Enhanced Border Security and Visa Entry Reform Act

Spanning all modes of transportation, the Enhanced Border Security and Visa Entry Reform Act requires all travelers through U.S. Ports of Entry by October 2004, to verify their identities via biometric reference to their travel documents. The choice of biometric on travel documents, while open to further discussion, would need to be supported by domestic U.S. and international standards bodies. Given the nature of the law enforcement infrastructure and related back-end databases, this biometric requirement will be satisfied, in the foreseeable future, by fingerprint templates, digitized photographs and, in some cases, by iris and hand geometry templates.

In effect, the Border Security Act provides a focal point for identity verification and access control, since the document checking processes at ports of entry affect airline workers and travelers, truck and automobile drivers as well as seafarers and sea travelers.

The U.S. portion of the North American transportation worker population needing identity cards is estimated to be about 15 million persons.

Documents issued to workers and travelers must be read by a finite set of readers.

How the identity verification process for travel documents and worker badges and licenses is coordinated and standardized becomes a very important question for buyers and sellers of technology and access control systems.

2.3.3 State Government Legislation

California has long been a legislative “bell weather” for the nation. The following areas of California law exemplify the types of privacy and fair information practices laws being enacted around the nation.

- Constitutional Right to Pursue and Obtain "Privacy"
- Consumer Credit Reporting
- Social Security Number Protections
- Medical Information
- Identity Theft
- Control of Personal Information
- Unwanted Calls, Mail, E-Mail, Faxes

For more detail, see Appendices D and E. The compilations in those appendices illustrate the depth and scope of this body of law, and possibilities for future action.

2.4 Public Sector Executive Activity

2.4.1 Federal Executive

The federal government is now engaged in a large-scale effort to build a strong authentication capability to support e-government. Expanding e-government to enhance citizen-centric government services is a key initiative of the President's domestic management agenda. To advance this agenda, the Administration established the E-Gov Task Force in July 2001 under the Office of Management and Budget (OMB). The Task Force identified the key e-government initiatives across the federal government best positioned to support the management agenda. The President's Management Council approved 24 initiatives in November 2001. These 24 initiatives defined government services and business transactions within four segments: citizen, business, government, and internal operations. All of the initiatives represent cross-agency efforts and are targeted for implementation within 18 to 24 months. In addition, all require some degree of authentication to support some or all of the business services and transactions. It is recognized that the four segments have different characteristics, and thus different authentication requirements. To support the needs of all of the initiatives, the E-Authentication Integrated Project Team, managed by the General Services Administration was directed to provide common authentication services and infrastructure, and enterprise architecture support. To accomplish this, the E-Authentication Team, plans to build and operate a Web-based e-authentication gateway. The gateway will provide common authentication services and single sign-on capability for all e-government services. The objective is to provide a set of common, shared services that all federal agencies can use for authenticating the public.

The federal government has issued an RFP relating to the creation of this e-authentication gateway. This system will create a trust system based on standards relating to enrollment, credentialing and authenticating individuals and methods of sharing the information across identity service providers. Once operational identity service providers, governments, agencies, departments, businesses and other organizations are allowed to apply for inclusion, the processes employed for identity functions will be reviewed and certified to meet minimum standards. Users of the gateway will be able to receive sufficient information to ascertain how to trust the enrolled identity service providers, thus precluding the necessity of developing and operating additional identity systems (for more information, see www.cio.gov and www.egov.gov).

2.4.2 State Executive

There is significant activity afoot among the states in the arena of authentication and identity management. The following is intended as an illustrative example of two such approaches at the state level, and not as a comprehensive survey. The state of Iowa’s approach is treated in somewhat more detail because of the problems and prospects associated with creating a single “core identity.”

2.4.2.1 State of Massachusetts

The commonwealth of Massachusetts is developing a centrally supported identity service, which will support many different levels of single sign-on enablers, from username and password to other, higher-level methods. Massachusetts state government has also recently gone through an enterprise-wide review and comprehensive drafting of privacy policies appearing on the Web sites of state agencies and departments.

Massachusetts values the right of citizens to maintain more than one electronic authentication that remains unlinked to a single or related set of databases. In fact, during the design phase of the Massachusetts Government portal's centrally supported identity service, it was specifically determined for legal and policy reasons to require Massachusetts state government employees, who are also citizens of the commonwealth of Massachusetts, to use two different electronic identities – one for each role. It was determined that using the same username and digital identity for employee and citizen transactions was against public policy and opened the door to abuses in the arena of privacy, fair information practices, and other liberties.

2.4.2.2 State of Iowa[3]

Iowa has begun an innovative Identity-Security Project[4]. They are working to create a clearinghouse where the various documents used to create identity (birth certificate, death certificate, driver's license, marriage license, and social security number) can be linked. Then mechanisms can be developed to track attempts at identity theft as well as allow agencies to cross-link identity verification. Perhaps the citizen will eventually be able to update his identity information across a range of participating agencies with a single change.

At the point of issuance for a social security number and DOT-issued driver's license/identity card (hereafter called ID), the birth certificate presented as proof of identity could be referenced against a state birth certificate database. If the birth certificate is valid and no other ID's have been issued from it, the birth certificate would be linked to ID's issued from it. The birth certificate record would also be electronically tied to the DOT photo database.

This has three advantages:

- When an ID is then presented in certain situations calling for strict security, a check could be run against the face database stored by DOT and identity could be established (i.e. airport counter).

[3] http://www.iowaccess.org/government/its/News_Items/Draft_Identity-Security_Project.htm
[4] http://www.iowaccess.org/government/its/News_Items/Draft_Identity-Security_Project.htm

- Only one ID would be issued per birth certificate. This would allow easier identification of individuals attempting to falsify identity if the birth certificate is presented a second time.
- Enhanced procedures will lead to a decline of identity theft and fraud.
  The end result would be a system that incorporates individuals, picture ID, processes, documentation and identity.

Assuming that creation of a common identification system is possible, the key to mapping identity with roles in a range of distinct communities remains[5]. After proper identification, additional constraints are likely to exist; in fact, the constraints may be the key reason for the identification. (It's my bank card but I can't use it if I'm overdrawn; it's my driver's license but even I shouldn't use it without wearing my glasses; it is my employee smart card but it doesn't get me through most secured doors because I still don't belong there.)

It is role-based identity in a particular community that leads to an authentication that allows an authorization for whatever access or action is desired. As Iowa already recognizes, care is necessary to avoid building in single points of failure across the range of communities. Iowa contemplates an identity revocation process triggered by a death certificate. This requires some thought about how to keep from incorrectly cascading the greatly exaggerated rumor of the death of Mark Twain through a common identity system. It is fruitless to cancel his bankcard, phone card, social security check, HMO eligibility and payroll check before the death is confirmed as *the* Twain and not someone with the same name and birthday.[6]

Iowa's approach may be an excellent foundation for such a system. As the Iowa approach illustrates, government's role in creating an identity system is to concentrate on the "who" someone is while others (businesses, associates, social organizations) who interact with the person determine the "what" that someone is. Trust builds from their interaction with the person, not from knowing "who."

There are some states that may not (i.e. currently disinclined or legally constrained) participate in even this level of blending government and commercial identities. A discussion on this that recognizes the diversity in state governance needs to occur.

---

[5] ("Yes, that is my credit card within the U.S. banking system and yes, that is my driver's license within the state motor vehicle and driver registration community and yes, that is my badge / employee # / smartcard / etc. within my employer's community.")

[6] The Belinda "twins" of Australia – same name, exact same birth date lead frequent confusion. http://catless.ncl.ac.uk/Risks/17.88.html#subj1

3. Approaches

There are several ways to look at approaches to identity management. One may look at this question as a matter of policy and law (e.g. privacy legislation, policies requiring use of a single username, etc); or as business cases and practices (e.g. prioritizing and selecting identity-related methods based on costs, benefits and risks); or as technical architectures and technologies (e.g. a global public key infrastructure, an inter-enterprise single sign-on, etc); or even at guiding philosophies and principles (e.g. "government must protect it's citizens life and safety as a first priority," or "the power to give, change and take a name or identity is the power to control"). To simplify the questions involved, it is useful to break the possible approaches into three basic possible directions.

A. National ID: Start Building Single ID, and Hope Problems Can Be Solved Later

One tech direction state policy makers could follow would be to start building a single citizen "core ID" system and rely on later solutions, such as better technologies and modified internal controls and laws to prevent unauthorized access controls, misuse, mistake and abuse. These threats are understood to be continuing concerns plaguing all available alternatives at this time.

B. Clustered ID: Single ID for Clusters of Related Transactions, but Allow More than One Cluster

Another direction would be to move forward with ID management projects but to specifically allow or require more than one ID – as opposed to a single core ID. This would assure that no single identifier can follow citizens around everywhere. The theory here is that people should enjoy the ease of single sign-on type access across government, or across businesses they commonly transact with, but a single ID is neither necessary nor desirable due to the underlying privacy and liberty concerns it raises.

C. Delay: Postpone Commitment to Decision Until Problems Better Addressed

Another approach would be to delay committing to any large-scale identity management technology, methods or projects until the privacy and liberties protections have been addressed to the point of being able to be designed in from the start. The theory here is that a bad solution rolled out prematurely may do more harm than good.

There are many ways to facilitate action toward options A and B. Eventually, creating an association of states to work on cross-border issues in conjunction with each other will be a necessary component of either of these options. There

is a lot of precedent for these sorts of aggregations of states, including the Electronic Benefits Transfer Council of NACHA, various multi-state compacts for dairy policy and group purchasing of goods, and regional planning authorities. Even the Western Governor's Association is a type of multi-state operational authority, running a college and other operations.

However, to follow option B alone, it may not be necessary to work at a multi-state level if none of the systems facilitate cross-state-border transactions or pass through of user identity. Many existing state e-government portals, which allow for single sign-on by a citizen in that state, are example of option B. Similarly, virtually any implementation of the Liberty Alliance specification would be an example of option B.

3.1 Single Federal National System

Larry Ellison, CEO of Oracle Corporation, among others, has promoted the creation of a national identity card system. This would be a federal/core identity under option A. Under Ellison's proposal, millions of Americans would be fingerprinted and the information would be placed in a database used by airport security officials to verify identities of travelers at airplane gates. The federal government would develop the infrastructure, processes and policies to create a single national identity system. Most of this system would have to be developed anew. Similar national government-based approaches have been employed to some level of success (as well as failure) in a number of other countries, but could face substantial resistance in the United States.

3.2 State Federated System

State governments could produce a federated system. Such a system would leave the basic identity related decisions to the states. Such federation could have as a goal the achievement of a single citizen ID, under option A, or the facilitation of certain clusters of ID, under option B. Under option B, for example, it is possible that the federated state system would focus only on an ID that citizens use for state government transactions and other pre-authorized transactions with other levels of government, other state governments or private entities that have joined the federated club, agreed to any applicable rules, and use interoperable systems and business methods. Such a system could exist contemporaneously with a federal government system and other private systems. Eventually, these systems could be linked or they could remain unlinked. It would be important to respect the choice of the person identified when determining whether to link ID systems in which that person participates. However, if a federated system were to proceed explicitly and deliberately toward option A, a single ID, then the mentality of such an architecture would probably not require citizen input in the linking of systems. To the contrary, the ability to link all ID systems to a common core ID would be the basic point of any option A design.

A state confederated identity system is one that would rely on each state managing its own identification system for its citizenry while involving dynamic collaboration among states to achieve the common goal of maintaining reliable identity creation and credentialing systems. The value such a system could provide is in the establishment of sound policies, procedures, practices and guidelines for an identity management that can be leveraged with confidence among various levels of government and the private sector. At present, there is no real organized effort to establish such a system among states.

Part of the reason to federate among states is that the U.S. identity-credentialing system, at all levels of government, is not keeping pace with the twenty-first century citizen. At present, states or their respective local governments are responsible for maintaining birth and death certificates (and other health records), and, most importantly, vehicle driver and non-driver licenses. Each of the 50 States has established its own mandates for what areas of government are responsible for these foundational identity documents and their respective business processes.

An organized, confederated system would not necessarily have as its goal, to establish a single business model across all 50 states. Rather, it could allow states to maintain their own processes, yet establish criteria to provide consistent levels of trust in the various credentialing systems that states have established. Determining exactly what metrics would result in such trust, however, would be a considerable undertaking, but one worth investigating.

The inconsistent array of business processes and system designs that were developed and expanded with mid-twentieth century business logic is the basis for the inherent weakness of all government identity credentialing systems currently in place. Collaborative efforts by states would need to focus on improving this model from a global village and Internet economy perspective. Such an expanded view could have a positive impact in support of homeland security, law enforcement, and electronic government service delivery.

Some amount of collaboration needs to exist in order to support the degree of mobility available to citizens of this country and of others as well. A confederated organization of states, to facilitate foundational identity management, would have the power of consistent thinking and planning but would likely need individual state legislated funding, or homeland security imprimatur and funding, or other federal funding.

For a state federated solution to succeed there would need to be substantial agreement and cooperation among states to develop a great deal of commonality in the procedures, policies and technical implementation of states' systems. Building upon existing infrastructure and processes, state governments could work cooperatively to develop standards for enrollment, credentialing and authentication to produce a state-based identity system. State governments

could adopt or create a process for developing, agreeing to and implementing their individual components of the federated system. See Appendix F for more detail on an "Operating Rules" approach to achieving such cooperation and agreements among states and partners.

3.3 Systemic Uniformity: Part of the "Management" in Identity Management

One of the key outcomes of a state federated approach would be to establish uniform system standards. As stated in Section 2.1.1 of this report, it is clear that there will ultimately be a demand for cross-sector (public/private) interoperability, and that common denominator solutions will be required. Any common-denominator solution should be consistent with the vision for identity management stated in 1.1. In summary, an identity management system should support common identity needs of governmental and private transactions; reduce costs and/or enhance service quality; safeguard the health and safety of the public; and preserve or improve individual privacy. Support for the identity needs common to the public and private sectors can be achieved through uniformity – uniformity in technical standards, business processes and responsibilities. Uniformity also helps reduce costs by facilitating the development of plug and play equipment and systems that can be used by multiple jurisdictions or companies. The competition fostered by uniformity leads to cost savings when contractors are bidding on open, standards-based systems, rather than on closed, proprietary systems. Privacy can be better protected when there are uniform design requirements to protect personally identifiable information. However, a uniform system, once broken, can also be the biggest enemy of privacy and security. Clearly, uniformity is the basis for both options A and B. It is also the basis for system interoperability.

There are a number of options for achieving system uniformity and interoperability. These options entail various approaches to the question of governance, which is discussed in Section 5.2. One governance option for achieving system uniformity and interoperability is the single, national ID envisioned in option A. Option A is uniform by its singular nature. Another option would be for the federal government to unilaterally require uniform standards, business practices and responsibilities. Other options are more cooperative in nature. Cross-state coordination could be achieved through a state confederated identity system, as described in 1.40 of Appendix F. Cross-state and cross-sector coordination could be achieved by the Public/Private Consortium Identity System described in 1.41 of Appendix F.

There is another option that governments could choose. Do nothing. Assessing the environment could lead decision makers to decide for many reasons that this is not something that should be dealt with by government. The private sector might solve these problems. Current fiscal conditions require attention to more pressing priorities at this time. This is not a responsibility of government. The time is not right. The potential political consequences are too severe. And, perhaps most importantly, a later time may yield adequate solutions to the

privacy and liberty challenges posed by linking identity systems. All of these and many other reasons could lead to a decision to not take action in this area.

4. Analysis

4.1. Identity Systems Are Not Homogenous Because Identity Is Not Homogenous

Clearly, the concept of identity is far broader than the mere content of a name. While names and naming protocols are a critical element of identity, in that they give us the means to call out one identified individual from another, the underlying relevance, role, context and meaning attributed to a given named person can only be gleaned by reference to other factors. The full measure of identity of an individual is a subtle and multi-faceted complexity. This is because people exist in many social, economic, political, cultural and other dimensions all at once. In short, one size does not fit all when it comes to the full identity of a person.

4.2. Factors to Consider

When evaluating the cost, benefit and risks of a planned system of identity management, it is critical to consider the scope of the system. The availability of technologies using Web browsers tempts planners to assume that a system can and will eventually be used by everybody, everywhere. This assumption should be challenged because it carries with it much in the way of business, legal and policy baggage. The broader a system of identity, the more complexity, expense and potential exposure to liability flows from it. Beyond those practical considerations, deeper governance and policy implications also lurk just beneath the project plan.

The following diagram illustrates domains of authentication and identity management from an institutional and organizational perspective. The smallest oval in the middle depicts an intra-agency system for authentication or identity management. Such a system would probably include only employees and/or contractors in one part of a larger agency. You can imagine an e-mail system, set of project management applications with user accounts linked to the e-mail, and an intranet for discussion also linked to the same authentication of users. People who operate in teams on projects and use group-ware benefit from linking identities across applications in this manner.

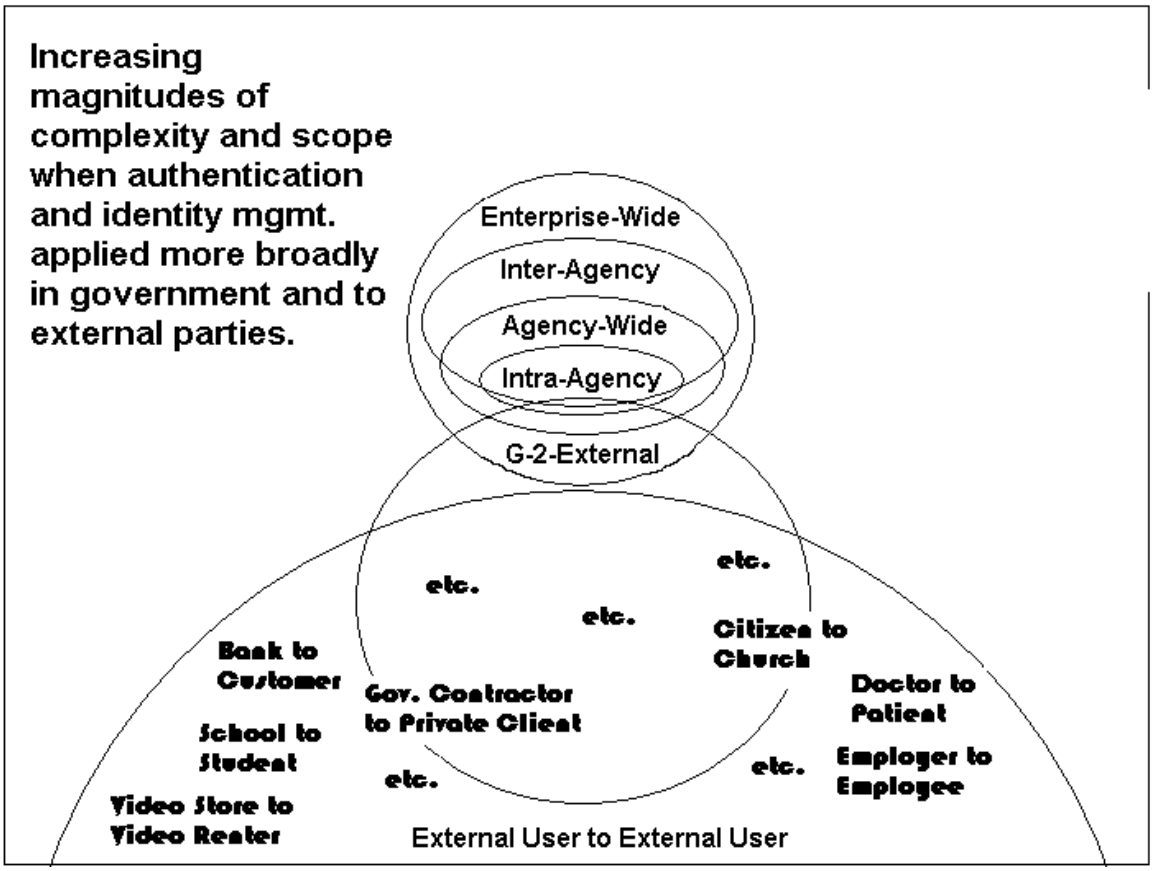
The next level up is the agency-wide application, which is similar to intra-agency, but includes everyone in the organizational unit. Common e-mail systems are the best example at this level, as well as the inter-agency and enterprise-wide levels. Inter-agency applications may include all or only some of the constituent agencies, which is why the oval does not subsume the entirety of the agency and

sub-agency ovals. Enterprise-wide identity systems, by contrast, are larger and cut across all lesser-included subdivisions at the agency, department or unit levels. The orders of magnitude of complexity in getting more than one agency to use the same systems, business processes and command structure necessary to enable such systems is far in excess of what is necessary to accomplish the same plan at the sub-agency level among colleagues. This is because the business units involve people who are on the peer level and who frequently have different business objectives and processes that must be respected. Someone – or everyone – must change to accommodate these new types of systems. This, among other things, causes additional difficulty, which is magnified at the enterprise level of planning and requires direct leadership and intervention in order to be accomplished.

All of these increasing levels of hardship, however, pale in comparison to what occur when systems of identity and business processes from internal operations come into contact with those from external entities. Whether those external entities be other states, other levels of government or private sector organizations, they all present difficulties. Of course, when the other levels of government are localities that can be directed to act by the state (as is the law in some jurisdictions), the difficulty is greatly reduced. In fact, it is a qualitatively different type of difficulty, because there is a hierarchical relationship that exists and one party can demand action by the other. By contrast, when an organization like a state government seeks to create an identity management system with an external organization that it cannot directly control, like another state, a private company, or even a cluster of companies, then a strategic approach is needed. The interests, preferred technologies and approaches of the other parties become critical to accommodate. Similarly, the underlying rights and obligations flowing from identity control will need to be apportioned among the stakeholders along with a clear understanding of corresponding responsibilities, suggesting the need for a federated system of some kind rather than a command and control system.

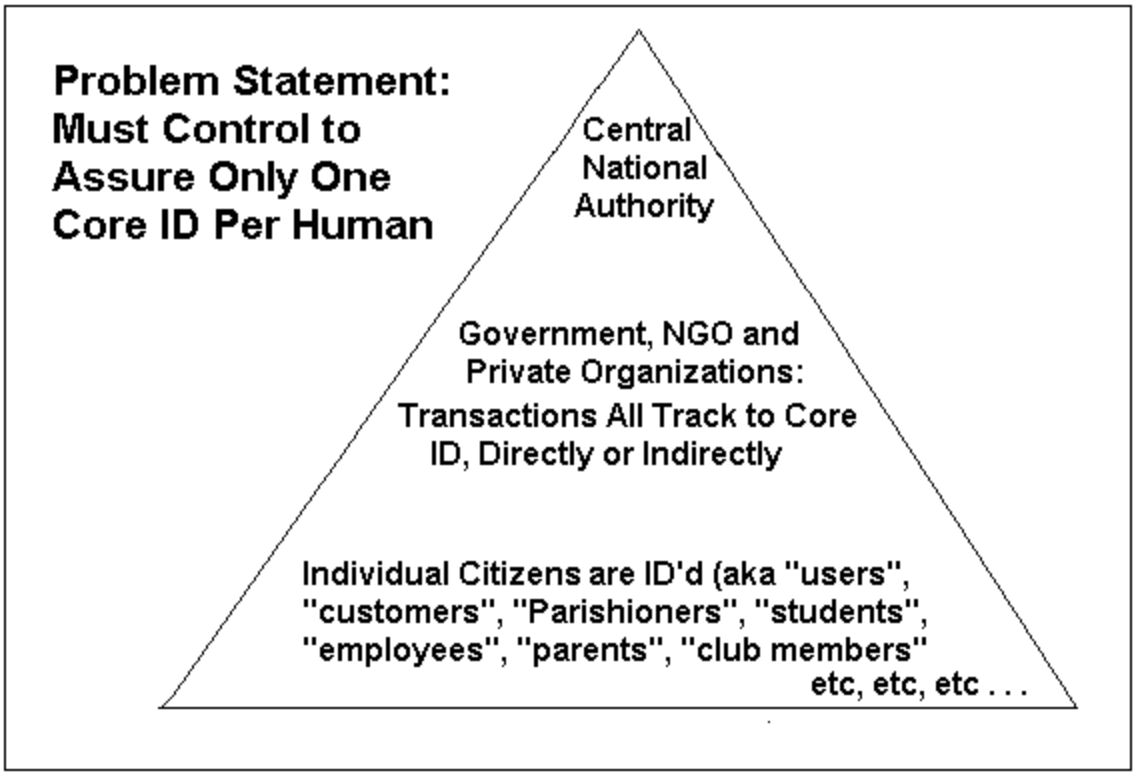
Notice that the government-to-external systems (g-2-external) involve two ovals that can be thought of as equally large (or perhaps the external system is larger, in that it cannot be “ordered around”). Nonetheless, assuming there is some specific business reason for the government and external systems to interoperate, then it is possible to assign a value to the benefit of that synergy. For example, if each organization saves $100 million, then even a few million dollars in cost and hassle in combining the systems may be worth it. More typically, while technology makes many interoperations and shared identity transactions possible, the business and legal demands that must be answered make it infeasible. In addition, it is necessary to create governance layers to manage such inter-enterprise systems, whereby the stakeholders all have a proportional voice in developing the structure and rules. This means it is best to only attempt planning identity management systems when there is a clear business case for them, and to leave more global systems for future phases of

development when more is known. Notice also that the creation of an identity system by government that would be used by purely external parties can be seen as much larger than state government and immeasurably more complex and difficult to create. Arguably, such systems should be the result of many more decades of experience and practice rather than built now, in advance of the business, governance and legal regimes necessary to support them.



Governance will be another key factor. As states begin to transact using electronic authentication with other governments or businesses of equal or greater power and authority, it will not be easy to simply demand that a certain system or method be utilized. Rather, it will be necessary and desirable to create voluntary associations or organizations that agree to share identity and other business information about customers, citizens or other individuals, and to establish voluntary agreements governing such matters as the types of opt-in agreements needed by end-users, joint venture terms, voting rights, liability apportionment, technical standard setting, and other practical issues that arise. These types of issues are treated in Sections B and D of The National Automated Clearing House Association's CARAT Guidelines (see www.nacha.org).

Consider the following diagram, which provides a more explicitly visual statement of the presumed model of a core identity as part of identity management. In this model, while people may continue to enjoy several different identities, every ID must track back to a single core identity. The model assumes that all sectors of the economy and society will operate by or on behalf of a central identity management authority of some kind. Such a central authority would be responsible for providing the technical and business rules whereby all other identity systems are capable of interoperation and traceability back to each user's single core ID.



Such a global system, while potentially attractive for certain commercial and law enforcement applications, carries with it tremendous hurdles. It is, in effect, the eternal to external problem illustrated in the previous diagram.

4.2.1. The Context in Which Identity Arises

Once a particular project involving an identity system is on the drawing board, perhaps the more important factor to consider when fashioning the approach is the context in which the need for identity management has arisen. The first and most critical factor is whether the vantage point from which the question is seen is that of a central authority, an individual or an autonomous group. Depending upon the point of view, dramatically different problems are assumed, and hence different and potentially conflicting approaches appear appropriate. Of course, it is possible for a central authority like a state government to try to see a given

problem from the point of view of an individual citizen or an independent group. However, it is more typical for a government to see issues from the point of view of its own operational convenience and institutional policy imperatives. Nonetheless, each of the following three possible perspectives is drawn with the context of state government policymakers in mind.

4.2.1.1. Central Authority

From the point of view of a central authority, there is logic to being able to assign identities and control them according to hierarchically managed rules. An illustration of this is the desire to create a single core identity, to which all other identities correlate and to assure that such correlation occurs according to centrally mandated rules. This allows for an arrogation of control and decision making at the institutional level. An example of this would be the issuance of an employee identity card or a national identity card. In either case, there is no need for a physical card, the entire system can be tracked to a password, a software token like a digital certificate, or a biometric measure. Such centralized ownership and control allows for efficient delivery, modification, authentication, tracking, and termination of the identities.

A state government seeking to support the centralization of authority for identity management would create requirements or incentives for every individual to be issued a unique identifying number or other token and would allow for all other individuals or organizations to use that same unique ID, according to a single set of rules. Ideally, there would be a single ID per citizen at each state, and thus at the national, level. This approach would first commit to or set in motion the creation of such a system, and would subsequently attempt to moderate the as yet unsolved challenges posed by such a measure to privacy, individual liberties, and independent group autonomy.

4.2.1.2. Individual Citizen

From the point of view of an individual, there is logic to being able to individually manage the various existing identities, tokens and authorizations that one has. One illustration of this is the desire of people to go by a nickname for their local political career, a professional designation for work purposes for their work, and a stage name for their hobby rock band to keep a healthy distance from infatuated fans. There may be an understandable desire to maintain a wall of separation between different identities by using different e-mail addresses, business cards, stationery, mailing addresses, and other identity credentials for each name and corresponding realm of identity. Another illustration of this is the desire to create a personal file containing all the various passwords, usernames, system preferences, and other relevant information needed to keep straight all the identity systems in which a person participates. Examples of this would be the user names and passwords so many citizens now possess for their work, family and banking activities. From the perspective of American political history, it is clear that a deep respect for individual liberties and civil rights animated much

state common law and both federal and state constitutional law, including recognized legal holdings supporting a citizen's right to wide discretion to manage an identity or to use anonymity as desired. See Appendix B for more details.

A state government seeking to support the rights of individual citizens to own and control their own identity in its many manifestations would seek to preserve or restore time honored state based sources of common law respecting the rights of individuals to name themselves, to change their names on their own accord, to select any name – including unorthodox syntax and formats, to maintain more than one unaffiliated name and identity when there is no intent to defraud or commit other crimes, and to eschew the use of any identity when engaging in anonymous speech or conduct for political or other legal purposes. In addition, a state government seeking to support the continued rights of individual citizens to make up their own minds about their identities would delay commitment to a technical or business architecture for centralized identity management until it could be demonstrated that such a system would not relegate these current rights to the annals of U.S. history. Support of such decentralized technical architectures as P3P and the Liberty Alliance specification would tend to align with this point of view.

4.2.1.3. Autonomous Group

From the point of view of an autonomous group, there is logic to being able to remain independent of other identity schemes used by other groups. One illustration of this is the case of a political or social group that seeks to maintain the privacy of its member's affiliation with that group. For example, the Supreme Court has ruled in NAACP v. Alabama, 357 U.S. 449 (1958) that members of such groups need not identity themselves publicly with the group, that the group need not turn over membership lists such that individual participants can be identified and correlated to other identity systems, and that freedom of association requires that government respect these boundaries.

Another example would be a corporation that seeks to maintain a primary and exclusive relationship with its customers or other business affiliates and who therefore desires to use naming schemes and identity methods that are deliberately different from those used by other organizations or national systems. A simple example of this is the deliberate walls erected between various mainstream "instant messaging" systems today, preventing the recognition of a user identity from one system to another. Of course, depending upon conditions in a particular market, a given business may determine that it is a better decision to use identity and naming schemes that are common among certain other businesses (such as in the case of an affinity partnership of related services, or some other federated identity scheme). However, the occasional existence of such fledgling systems of shared identity information and methods does not reverse or eliminate the fact that other (perhaps most) competitive contexts reward maintaining different identity systems.

State government decision makers seeking to support the continued ability of autonomous groups to create and manage their own competitive or proprietary identity schemes for their members would prevent agency functionaries from creating systems that pressure or require regulated companies, local governments or other governmental partners from using government-recognized naming schemes or methods that track back to a core identity for each individual. In addition, decision makers would likely recognize that there are legitimate and continuing business, political, legal and policy reasons exist for various organizations or other associations to have independent and non-externally-linked systems and methods of identity for their members or other participants.

4.2.2. Policy and Political Synthesis

The ideal decision making approach toward technical and business architectures for managing individual identities would take into account each of the three perspectives previously mentioned and would respect the underlying objectives sought in each case. Today, there are various technologies and proposed approaches to identity management that reflect and support each of the three perspectives and many others besides. As events continue to unfold and new innovations in technology and business practices are invented, more options will become available to policy makers. In the meantime, it will be necessary to more actively and consciously weigh the importance of different values and principles when selecting from among existing options or deciding to defer commitment to a solution until a later time.

States have always been the laboratories of innovation when it comes to experimental policy, technical and legislative approaches in the United States. In the arena of identity management, it is predictable that again states will continue to provide a multitude of creative and worthy options in the competitive marketplace of ideas as our nation struggles to evolve a broader approach to the identity conundrum. As these competing approaches are attempted and implemented, time will reveal the relative weaknesses, opportunities and strengths associated with them – both individually and in combination. States can move at a far faster rate of speed than the federal government, can track best practices in the private sector more completely, and are more sensitive to regional and local needs and possibilities than is any single national or multi-national organization in the public or private sectors. These unique and wonderful advantages inherent in this level of government will serve the nation well over time, and will provide a ready arsenal of potential for the legislative, judicial and executive stewards of our state governments.

4.2.3. Drill-Down: Central Authority E-Government and Citizen Identity Perspective

Most of the analysis in this section assumes the creation of identity systems for e-government initiatives and citizen-identity schemes for particular applications, such as voting. When establishing the relevant factors to assess in development of an identity system in state government, it is necessary to first consider the scope and boundaries of the uses to which that system will be put. For example, the following types of applications each carry with them profoundly different and sometimes conflicting legal and practical sets of requirements:

- Political Activity
- Public Records
- Social and Cultural
- Religious Affairs
- Personal, Family or Household Uses
- Business Transactions

As noted elsewhere in this white paper, political activity carries with it many legal and constitutional protections for the privacy and sometimes even the anonymity of the citizen. For example, the right to publish or speak anonymous political statements has long been recognized under the U.S. Constitution and the constitutions of many of the states. Similarly, certain systems raise unique technical requirements, like the need for secret ballot functionality for any electronic voting system. In addition, some states, such as the commonwealth of Massachusetts, have statutes restricting certain information from appearing on the rolls of lists of residents that are used for political canvassing, including the names of minors living in households. Systems being used to support personal, family or household interactions will likely implicate any number of consumer protection laws and regulations, some of which require special electronic signature agreement and notice functionality or trigger mandated controls over the use and sharing of personally identifiable information.

In the arena of business transactions, there are perhaps the fewest numbers of issues raised. In addition, the clearest near-term economic and political drivers are at work to encourage implementation of e-government systems to enable online business transactions such as filing of taxes, applications for grants, administration of benefits, procurement, licensing and permitting processes. For these reasons, the following analysis assumes that the policy maker is considering creation of an identity system to support e-government business transactions and not the broader and far more problematic issues raised by creation of a state affiliate to a single citizen ID that can be used for any or many purposes within or outside of governmental transactions.

4.2.4. The Nature of Transaction

Given the reality that for the foreseeable future there will be a multiplicity of electronic identity systems operating within, between and under the legal authority of state governments, it is useful to consider the specific types of transactions to which a given system will be put when determining the applicable technical and other requirements and constraints. Some business transactions require, for example, less security than do others. Similarly, some business transactions may only require identification of a partner or regulated organization, which in turn vouches for the role or authority of its individuals but does not individually authenticate each one to external entities. Finally, some business transactions may not require authentication of any kind – organizational or individual – and therefore it will be possible to completely forego the cost and complexity of such systems as a prerequisite to enabling those transactions.

4.2.5. Regulation of Private Parties: Federal ESIGN Issues

Under recent federal law, use of electronic signatures has been legalized, but states are constrained to remain "technology neutral" when regulating online business transactions – such as banking transactions – with consumers and businesses or insurance company contracts with policyholders. The E-Signatures in Global and National Commerce Act (ESIGN) prohibits even the naming of a technical specification in such regulations. Reference to the Liberty Alliance protocols or the W3C Digital Signature specification could be preempted, under this law. However, there are various limits to this preemption – including the exemptions to the law for certain consumer notices, and the exceptions for safety and law enforcement. The fact of this federal preemption covering use of electronic signatures in global and national commerce is going to be an important statutory constraint for states to deal with as overall policy and legal architectures are considered for authentication.

4.2.6. Risk Management

The need for identity management derives, in large part, from the predecessor need to authenticate online users. The need for authentication, in turn, is a response to the need to avoid or reduce the risk that the wrong person will access, use, change, delete or otherwise improperly interact with valuable data or transactions. To fully understand the role of authentication and identity management, it is therefore necessary to regard these as part of a constellation of risk assessment and risk control measures.

There are myriad ways to approach risk management. For purposes of introducing the basic issues, we will use the Massachusetts Institute of Technology E-Commerce Architecture Program's (eCAP) Risk Management

Method for E-Government and E-Business. This method is currently under development as part of the ActuariNet research initiative of eCAP.

4.2.6.1. MIT eCAP Risk Management Method for E-Business and E-Government

In making a decision about whether a given online identification is adequate to permit a transaction, one must make a risk assessment. It is the unusual transaction that would require close to 100 percent certainty as to the identity of a party. Consider that transactions – even important ones – in the physical world are laden with opportunities for fraud, error and other confusions. Paper is not especially secure, as a technology. Virtually no system is immune to abuse by motivated people on the inside of an institution or process. In the end, there is no 100 percent solution to security. Rather, subtle judgments about acceptable risk must be made. This is certainly true with respect to online authentication of identity.

It should be recognized that risk assessment is fundamentally subjective. It is a reflection of how much risk the assessor is comfortable taking and how one perceives the odds and varieties of future possibilities. This is, in a sense, real guesswork. There are, however, predictive models that can assist. The best model is the brain of a person who is very experienced in a given field of activity and who can extrapolate from that experience. The insurance industry has done a good job of formalizing this type of experience into actuarial and other tables and models. In the end, however, much opinion and nuance is input into the risk management process.

Some state jurisdictions are frankly less tolerant of risk and fraud than others. Of course, the less tolerant of risk one is, the more one must be prepared to spend and do to manage the risk. Every state should apply risk management and principles of acceptable rates of risk, at a minimum, for transactions where only money is at stake. Other transactions that carry policy implications – like citizen privacy, or political implication are less easy to subject to a risk equation. Additional layers of security and controls may be appropriate based upon political and social values. These softer types of values can and should be assigned monetary numbers or other objective measurement as part of an explicit process of risk management.

The following process is one way to establish and manage risks of all types of systems, including authentication and identity management systems. This process was developed at the Massachusetts Institute of Technology's E-Commerce Architecture Program (eCAP). The eCAP research initiative, known as ActuariNet, explores methods to quantify, assess, avoid and manage risks resulting from e-government and e-business activities by addressing the issues at the design-phase. This method has been applied below to risks and scenarios associated with authentication and identity management issues.

The first step before applying this method is called “Risk Identification and Quantification” (e.g. spotting relevant risks and assessing the probability and severity of the prospective harm that would result, including the risk of initial mis-identification, the risk of later forgery or identity theft, and the risk of internal abuse). This initial evaluation must be done first, and then the following five steps can be applied and repeated until the risk is acceptable or it is determined that the plan is too risky to commence.

1. *Risk Avoidance* (e.g. Strategically choosing and structuring the business model or transaction types and technology selection in such a way that the business value remains but some of the identified risks are not implicated in the first place.)

2. *Risk Reduction* (e.g. Implementing the chosen business transactions and technology architecture in such a way that the remaining identified risks are mitigated in terms of probability of occurrence or severity of loss. Also known as Risk Mitigation.)

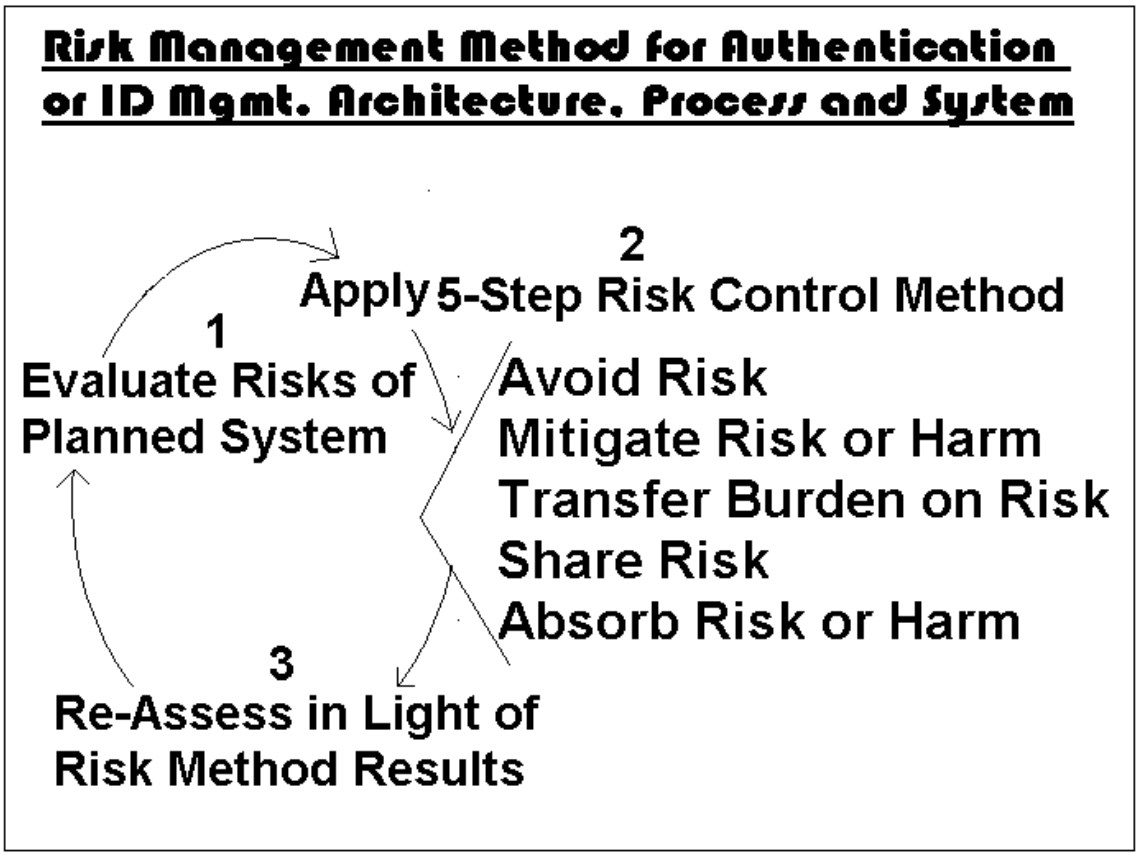
3. *Risk Sharing* (e.g. Creating a so-called “captive” – that is, a group of parties who shoulder certain risks and who are willing to fund a private group capital reserve among themselves to insure against those risks. This is a private, closed insurance pool. Note that unlike “risk transfer,” where the risk is shifted to other parties as completely as possible, with risk sharing all the member parties agree up front to contribute capital to the shared reserve.)

4. *Risk Transfer* (e.g. The most obvious measures include prior use of financial instruments like insurance or bonding and the use of contract terms whereby liability and other risk of loss is shifted to other parties. Risk transfer can also be accomplished by structuring the business in such a way that a different body of law applies whereby other parties are subject to certain risks without the need for private contracts [this “transfer” strategy is actually best accomplished prospectively as part of “risk avoidance”]. This strategy is also known as “shifting the risk.”)

5. *Risk Absorption* (e.g. Recognizing that the harm that would result from risks that have not been avoided, mitigated or shifted will have to be born outright. Strategies for dealing with this residual risk include the creation of strategic capital reserves or more formal “self-insurance” programs. Note that even if insurance or “captive” arrangements are made, the scope of the risks that are shared will still be limited in some way, and hence there will be residual risk potentially to be absorbed by any given party. In some situations, a state government will be immune to some legal liability based on the principle of sovereign immunity and implementing laws allowing capped tort claims. These types of limits

should be considered as part of initial risk assessment and when calculating remaining risk to be absorbed.)

The following diagram shows how to apply this method.



The above method can be applied to any potential system or transaction. When determining risks involved with authentication and identity management in a governmental practice and policy context, consideration of the following types of targets and harms are useful starting points:

- End-user (e.g. affecting a consumer or citizen): Identity error, misuse or abuse issues, such as identity fraud or the unauthorized access, modification, deletion or transmission of sensitive, high value or mission critical data and systems in commerce.

- Contracting party (e.g. affecting a vendor): Uncertainty regarding the integrity and authenticity of an electronic signature on a contract or other legally binding record.

- Business or governmental (e.g. affecting government Web server): Organizational identity misrepresentation or theft, such as by the redirection of Web traffic from the rightful owner's Web site to a fake site

for the purpose of harming the reputation or business continuity of the victim company and/or to defraud the users who were redirected.

- Critical systems (e.g. affecting police dispatch, airports): Illegal penetration or tampering with military, law enforcement, intelligence, energy, transportation or public health and emergency services systems or data in the public sector for the purpose of disrupting or degrading the core functions of government.

The arena of risk management is garnering a lot of attention as a critical element in the authentication and identity management puzzle. Among the relevant initiatives currently underway, it is also useful to consider the risk management process approach for authentication being developed at Carnegie Mellon University. This approach appears to rely more heavily upon facilitated sessions run by outside specialists and highly trained experts as part of the risk identification and assessment phase. For more information on this approach, see Appendix G.

For more information on the foregoing, please see http://ecitizen.mit.edu. Please note that the ActuariNet research initiative of MIT ECAP that gave rise to this risk management model is a work in progress, and the draft materials offered above are subject to change.

4.2.7. Latitude & Attitude: Differences in Risk Perception by Region and Jurisdiction

There are many examples of situations where different states may evaluate the same business transaction risks and solutions differently due to variations in priorities, sensitivities and policy values. For instance, in some states, there may be explicit “acceptable fraud” percentages that are assumed as part of a given transaction and for which it is determined that it would cost more money to prevent than the cost of the fraud itself. In effect, any state that accepts credit cards accepts such a view as part of the merchant fees paid into the risk pool cushioning the systems from repudiated transactions. In other states, local political determinations hold that no fraud of the public treasure is acceptable and extreme amounts of effort will be appropriated to prevent, detect and route out such activity.

4.3. Identity Management Principles

The advent of electronic technology for access and processing of information has created a sharp focus on issues surrounding identity and personal information. There are a number of key considerations or responsibilities attendant on any entity that undertakes identity management functions. Organizations planning for an identity management role should develop a base of principles around these key items to support the business requirements and determine the technical

requirements in the development of a system to fulfill that role. Some of the most important items on a list of considerations and responsibilities would be:

- Privacy
- Parsimony
- Anonymity
- Emergency response
- Law enforcement

"Privacy is a cherished American value, closely linked to our concepts of personal freedom and well-being." This quote is from a Memorandum for the Heads of Executive Departments and Agencies issued by President Clinton on May 14, 1998. The Clinton Administration undertook efforts to create policies and guidelines to direct the federal government and advise the country in the area of personal information. As decision makers undertake the development or adoption of privacy principles it is worth referencing prior work such as that of the National Information Infrastructure Task Force.

"In response to growing public concern, the Administration's Information Infrastructure Task Force (IITF) published Privacy Principles in June 1995 to guide future Administration privacy efforts. Developed with extensive consultation with the private sector, these principles were immediately endorsed by the private sector U.S. Advisory Council on the National Information Infrastructure" (Page 78. Access America, Reengineering Through Information Technology. Report of the National Performance Review and the Government Information Technology Services Board. Vice President Al Gore. February 3, 1997). That report stated principles for all National Information Infrastructure Participants, users of personal information and individuals who provide personal information.

Included in these principles were some relating to privacy, parsimony and anonymity. "Personal information should be acquired, disclosed, and used only in ways that respect an individual's privacy." (Ibid) "Information users should:

- Assess the impact on privacy in deciding whether to acquire, disclose, or use personal information.
- Acquire and keep only information reasonably expected to support current or planned activities." (Ibid)

Citizens can legally be anonymous in many situations. In situations when anonymity is not acceptable, then privacy and identity parsimony should be maintained to the extent possible. There are times when the realities of responding to emergency situations or law enforcement needs require some concessions to the preceding principles. Generally, it is easier to develop the guiding principles in cool reflection rather than in the heat of a moment of crisis. For more information on fair information practices, see Appendix E.

5. Conclusion

Reasonable minds will (and apparently do) differ on which principles should guide the policy, legal, business and technical architectures for identity management systems and practices. In the end, it will be necessary to devise innovative methods and approaches that support a balanced reflection of each of the competing interests.

In conclusion, it will be necessary for state decision makers to carefully consider the policy, technical, legal and business ramifications of identity management at the state level. The technical architectures chosen are not policy-neutral, in that they carry with them certain explicit or implied assumptions about the roles and expectations of users. In addition, the policy and legal approaches are charged with potential for missteps and controversy. However, it is clear that the basic drivers toward implementation of better identity management systems and methods will move states and other stakeholders toward creating more, bigger and broader systems.

In the end, it will be important to find creative ways to build the privacy, liberties and other policy imperatives into the systems at the design phase. In this way, the correct requirements for the systems are taken into account at the front end of the design process and are assured, rather than left to chance.

This page left blank intentionally.

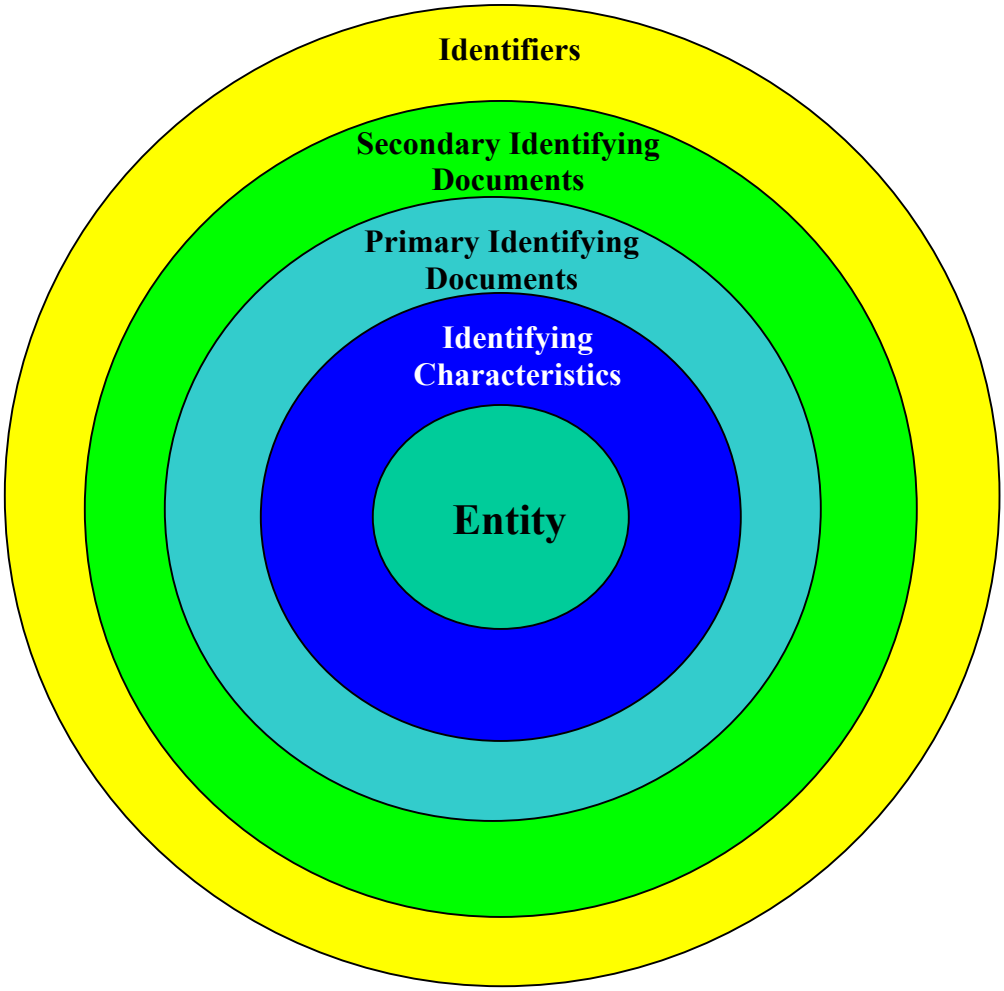
Appendix A

Glossary of Terms

By Ed Fraga

3.1 Entity

An entity is a being, a place or a thing



3.2 Identifying Characteristics

Identifying Characteristics are biometrics and other unique characteristics associated with an entity

3.3 Primary Identifying (or "Root") Documents

Primary Identifying Documents link an identifier with an entity often by association with an identifying characteristic such as a fingerprint.

3.4 Secondary Identifying Documents

Secondary Identifying Documents are standard documents referencing identifiers (such as a utility bill, bank statement or payroll check stub)

3.5 Identifier
Identifiers are names, numbers, titles meant to identify an entity.

3.6 Identification
A document that purports to be issued by an authority that has established the identity of an entity.

3.7 Identity
A set of identifiers associated with an entity.

3.8 Breeder Document

3.9 Credentialing
The processes of creating primary identifying documents, authenticating against those documents and issuing identification documents.

3.10 Authentication
Authentication is the means by which assurance of the identity of parties to a transaction is established.

3.11 Non-Repudiation
The assurance that the authentication of parties to a transaction is so “strong” that they cannot later deny that they were the parties to the transaction. If the authorization is very strong (like a biometric), then it had to be the person identified by the biometric who conducted the transaction. The evidence is so strong, the party cannot repudiate the transaction.

3.12 Trust
Trust involves our relying upon other people when there is a risk that we might be disappointed. When we trust someone, we make ourselves vulnerable to that person. Trusting involves taking a risk that one might be let down.[7][17]

3.13 Anonymity
Anonymity is the condition of being unknown or unacknowledged. The condition of an entity with no known identifier.

3.14 Pseudonymity
A pseudonym is an identifier of an entity assumed to disguise the true identity of the entity.

3.15 Alias
An alias is an identifier of an entity used in lieu of an established identifier.

3.16 Privacy
The assurance that information provided for a specific transaction will not be used by the recipient for purposes not authorized by the provider.

3.17 Security
Security is protection from intended and unintended breaches that would result in the loss or dissemination of data or the damage to the integrity, confidentiality or authenticity of systems.

3.18 Confidentiality
Confidentiality is the assurance that no one is able to eavesdrop on the transaction in progress.

3.19 Integrity
The assurance that the information received is identical to the information that was sent.

3.20 Authorization
The ability to determine what data a person has the ability to view, alter, create or delete and/or what systems that person has the ability to change.

3.21 Role-Based Authorization
Role-based authorization is a technique of authorization management in which individuals are granted authorization by assignment to one or more pre-defined roles. This allows understanding of their authorizations not by examining them in detail, but by knowing the authorization of these pre-defined roles.

3.22 Access
The method of getting to the information or performing the action. Access methods must be understood and adequately protect from inappropriate information disclosure or inappropriate ability to act.

3.23 System
An inter-related set of components arranged to accomplish a purpose. Components may include computer hardware, software, manual business processes, interfaces, etc.

3.24 Component
A portion of a system that has defined inputs, functions and outputs.

3.25 Computer Application
A set of computer programs and electronic databases developed and combined to accomplish a purpose by providing a given set of features, functions, and information products.

3.26 Interoperability
The capability of multiple components to work together.

3.27 Interface
A connection between multiple components

3.28 Integration
The connection between multiple components that allows for seamless sharing and communication to occur.

3.29 Digital Divide

The “digital divide” is the gap in opportunities experienced by those with limited accessibility to technology especially, the Internet. This includes accessibility limitations in:

- Social Issues (need to talk to a person, etc.)

- Cultural Issues (language barriers, etc.)
- Disability Issues (ADA, etc.)
- Economic Issues (access to technology devices)
- Learning Issues (marketing, overcoming unfamiliarity, changing habits).

3.30 E-Commerce

The use of communications technologies (such as Web-based technologies) for the conduct of business and service delivery transactions while leaving internal or external business processes substantially unchanged.

3.31 Computer Program

A set of instructions developed and put together to provide specific features and to perform one of more functions. Each program has input(s), performs action(s), and generates output(s).

3.32 Resource

Labor, capital, material or energy that is applied to a process to produce a result such as a product or service.

3.33 Workflow

A set of processes and activities that can occur in parallel or in sequence and are performed to accomplish a designated purpose and produce a given result such as a product or service.

3.34 Electronic System

An inter and/or intra set of related computing resources that are interfaced or integrated to provide certain features functions and information products associated with a given set of data and a given set of workflows.

Appendix B

The Starting Point: Common Practice and Common Law

Daniel Greenwood

[Please note that nothing in this article is intended or should be regarded as legal advice. Some material in this appendix and within the body of this white paper being are also being published as part of the 2002 NASACT/NECCC Leadership Book: *A Primer on Technology for Public Officials* and is a draft of a more formal article to be published in 2003. Suggestions, corrections or other reactions are welcome. The final version will be linked from www.civics.com.]

The advent of the networked age and ubiquitous computing is pressuring many areas of society to become more explicit about the existence, scope, meaning and usage of the otherwise largely implied depths of personal identity.

The status quo is that people are entitled to conceal their identity by being anonymous or to use other identities by using pseudonyms, provided they do so with no intent to commit crime or other frauds. Here is an everyday example: When walking into a store in the physical world, a person has always had the discretion to identify herself if asked, or to decline to identify herself. In fact, there is generally no rule against giving a pseudonym to a store clerk or anybody else when you wish to keep your real identity private.

This can be done, for example, to prevent people from knowing your home identity and risking unwarranted and unwelcome later contact from that person. Unwelcome later contacts could include unsolicited marketing or even undesired contacts by people seeking friendship or romance. At the extreme end of the scale, some unfortunate people require help from their places of work and government agencies to conceal their whereabouts and other personally identifiable information from disgruntled former employees or ex-spouses, stalkers or others who would do them harm. A milder example of lawful concealing of identity is the movie star who goes in public wearing a wig, using an alias, and trying to "keep a low profile." For a deep treatment of the laws and rules protecting the basic American right to remain anonymous or use pseudonyms, see Anonymity and Encryption in Internet Commerce (http://www.civics.com/content/cryptonon).

Here is the bottom-line: It is today the right of a citizen, absent a specific law to the contrary (as when exercising the right to buy a gun or when seeking a passport) to use any name they desire at any time, without government approval, unless they do so with the intent to defraud. This has been the basic "common law" rule for hundreds of years (if not more). For that matter, a person is still at liberty to indicate that they are simply browsing or "window shopping" when approached by sales staff and need not even provide a pseudonym if they so choose. There is generally no law against saying "thanks, but I'm all set for now"

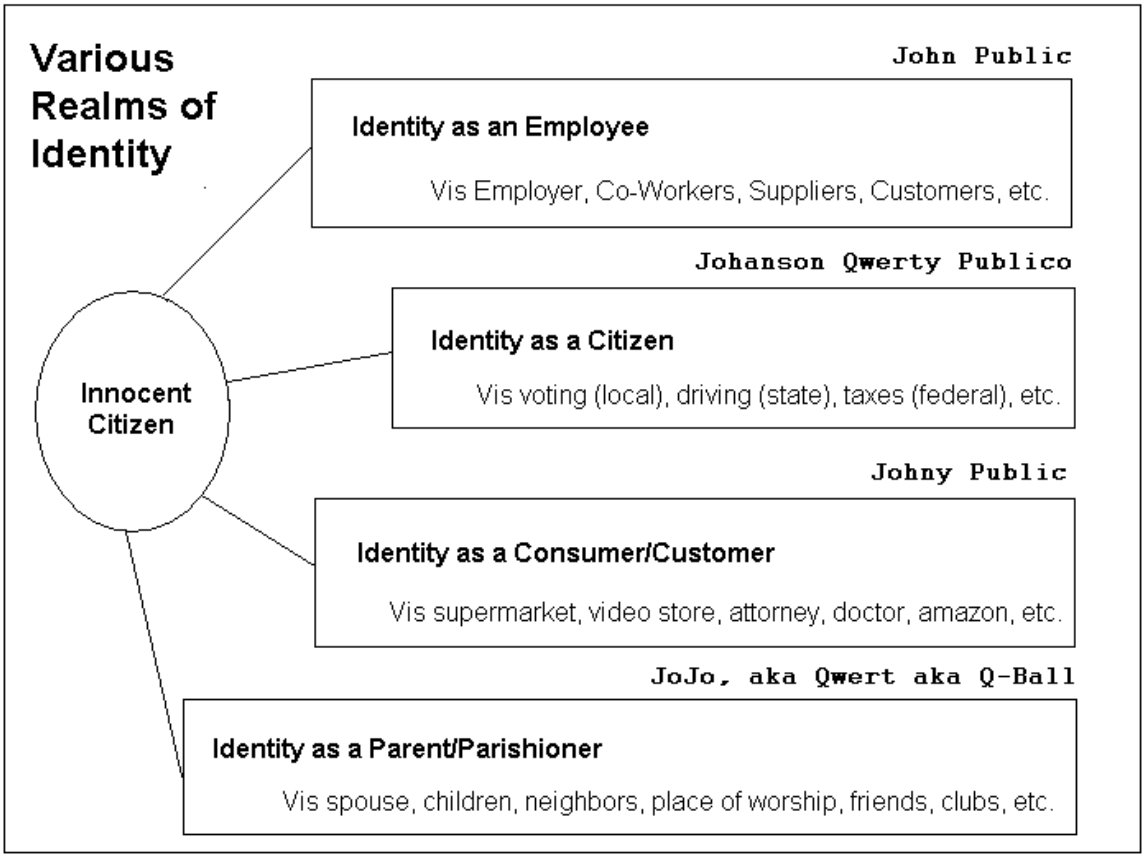
when asked if you can be helped, or if someone insists on wringing a name out of you, you are at liberty to use an alias.

Some exceptions to this basic rule, beyond fraud, include certain states which allow the use of aliases but require that additional names used for business be registered typically at a town or city hall. Another example of a spin on this rule occurs in states that require citizens to go to court to request a formal change of name. States without such requirements simply extend the common law rule, whereby anyone can change their name at will or use various names for various activities. States with statutes requiring a formal proceeding in order to effect a legal name change will also usually allow people to use other names even without specific approval. For example, in a 1969 New York court case, a judge ruled that while the petitioner was not granted a legal name change due to a technical rule, he was still at liberty to use his desired name in all the ways he had always done so. In that case, the person had been known by the single Sanskrit name Arindam for years by friends, family and business associates. In fact, he had registered for his social security and automobile club memberships under his chosen new name. This case demonstrates what little consequence a "legal" name change can have in states that require it as a formality. In a different court in New Jersey in 1996, it was ruled that a petitioner could effect a legal name change to a single name despite the record-keeping inconvenience to government agencies. In effect, the liberty of that person to enjoy a name change was paramount since, according to American Jurisprudence, the "state's computer programmers and record keepers were capable of adjusting their systems to accommodate unusual names."

Even in states that require formal name change or "doing business as" registrations for aliases, the Supreme Court has held that the general national rule is that any person may communicate political speech anonymously or with an assumed name. This freedom derives from the First Amendment and is necessary to prevent the chilling effects of having to identify oneself with potentially unpopular political views, possible retribution from employers or other personal attack. Whether a given state requires a formal proceeding to change "legal" name or not, people remain at liberty in general to use any identity they wish. When this liberty is coupled with the common practice of using cash to effect transactions in physical environments, it is easy to see how creating stricter management of identity poses challenges for policy makers.

Realms of Identity

The next diagram illustrates how the above policy and legal imperatives can be reflected by allowing multiple "clusters" of identity, but not creating or requiring use of a single "core" identity for each citizen. It shows the existing world of many identities held by an individual – none of which necessarily must intertwine with others.



The above diagram shows a type of user-controlled identity management that allows for many different types of systems and relationships, depending upon context. This approach is supported and reflected in the Liberty Alliance technical specification for identity. This type of technology allows for single sign-on across different enterprises by an individual, but linking identities would have to be done based on the consent of the individual and it would be possible to maintain more than one different ID. This is another example of how choosing a given technology architecture carries with it policy and legal choices as well. The Liberty architecture is a worthy first step toward creating better, more flexible methods of using today's legal and societal norms while also allowing better identity management from an individual and an institutional or inter-institutional perspective.

This page left blank intentionally.

Appendix C

Commercial Investment at U.S. Ports of Entry

By Jack Radzikowski

Overview

As the U.S. moves aggressively to control the access of individuals at ports of entry, there is a need to promote coordinated federal investments in identity document verification systems for workers and travelers across the aviation, highway transport and maritime sectors. Airline pilots, truckers, seafarers and private travelers, among others, should have to present a consistent set of credentials to gain access to both security-sensitive and other areas within port of entry facilities. Successful efforts to promote interoperable technology across federal agencies and their international counterparts will lead to quicker, more effective and less expensive deployments of technology. To attract investment in this emerging market, there are useful lessons for U.S. federal agencies available from the credit card industry; the experiences of other federal and state agencies in creating a market for electronic benefit transfer (EBT) cards, and; the Department of Defense Common Access Card.

This paper describes the framework of legislation that ties worker and traveler identification to port of entry access control; identifies the elements of a business case for attracting investment in commercial technology for these purposes; reviews important “branding” lessons from related credentialing efforts; and suggests some next steps for federal agency officials to consider in promoting timely, large scale deployments.

Legislative Framework

One common thread across Post 9/11 transportation-related legislation is the requirement for verification of the identity of individuals at security-sensitive, access control points. The Aviation and Transportation Security Act requires this for airline and airport workers. The USA Patriot Act requires this for hazardous material truck drivers. The Port and Maritime Security Act (awaiting House action) requires this for port workers and seafarers. These commercial workers must undergo fingerprint-based criminal history background checks and possess a badge that, in many cases, will be tied to the bearer via biometric comparison.

Spanning all modes of transportation, the Enhanced Border Security and Visa Entry Reform Act, (pending final Senate action), requires all travelers through U.S. Ports of Entry by October 2003, to verify their identities via biometric comparison to their travel documents. The choice of biometric on travel documents, while open to further discussion, would need to be supported by domestic U.S. and international law enforcement. Given the nature of the law enforcement infrastructure and related back-end databases, this biometric

requirement could only be satisfied, in the foreseeable future, by fingerprints and digitized photographs.

In effect, the Border Security Act provides a focal point for identity verification and access control, since the document checking processes at ports of entry affect airline workers and travelers, truck and automobile drivers, and seafarers and sea travelers

Documents issued to workers and travelers must be read by a finite set of readers.

How the identity verification process for travel documents and worker badges and licenses is coordinated and standardized becomes a very important question for buyers and sellers of technology and access control systems.

Elements of the Business Case for Investing in ID Verification Technology

The quality and cost of ID verification technology available to governments will be affected by the size and certainty of the business opportunity. The business opportunity, in turn, can be qualified according to the criteria listed below. An attractive investment involves a large volume purchase, on a date certain, with appropriated funds, driven by a legal requirement. Standardized technology allows for more competition and lower costs. An existing infrastructure suggests that the opportunity can be supported properly and that there could be interoperability across transportation verticals, and across ports of origin for travelers. An inclusive process for managing change sets the stage for the proper choreography among identity document issuers, card/document printer manufacturers, reader manufacturers, and system integrators when the time comes for large-scale deployments.

To the extent that these criteria are satisfied and the results made public, there is a higher probability of attracting the needed private sector investment and, consequently, successful deployments of technology.

1) **Volume**. Eight hundred thousand airport workers, 4+ million truckers, several million port workers combined with 24 million non-immigrant U.S. visas, and many millions of passports describes both a large opportunity as well as a serious problem of scale. The only example of commercial technology capable of handling such scale is in the credit card industry.

2) **Time**. Given that the legislated milestone for deployment of an automated border entry/exit system is October 2003, the time to begin federal procurements to support the event is now. Moreover, U.S. federal and state officials and port of origin authorities need to keep this date in mind as they make new procurements or amend existing contracts for identity verification.

3) **Money**. While substantial appropriated funds are available in 2002 and could be available in 2003, prototype estimation work based on commercially available technology needs to be completed before realistic cost estimates can be made. Estimates should include both the costs of standardized, commercial technology

as well as exception processing for authorities that choose not to proceed in a coordinated manner.

4) **Authority**. The Enhanced Border Security Act coupled with the related legislation affecting transportation vertical markets (mentioned above) provide sufficient authority for federal agencies to form partnerships with other public sector agencies.

In turn, the designated U.S. federal agency should use its delegated authority to recognize and participate in trade association efforts to standardize and certify technology (see 5 and 7 below).

5) **Standardized Technology**. Both the Patriot Act and the Enhanced Border Security Act recognize the importance of biometric technology standards for identity verification, remanding the choice of standards to the M-1 Committee (i.e. NIST, Justice, Transportation). The initial work of the M-1 is time limited by law. It should be extended.

6) **Existing Infrastructure**. Most commercially available ID enrollment and printing machines produce magnetic stripe and smart cards, 2D bar codes on paper or plastic documents and optical cards. The biggest customers, by far, for these machines are banks for credit cards and sovereign nations for travel documents. Assuming that the document choices of the biggest customers are proxies for existing as well as the next generation infrastructure, then 2D bar codes and smart cards will be the document media in most demand. This is because 2D barcodes can be printed to existing passports and banks are in the process of switching from magnetic stripe to smart credit cards.

7) **Inclusive Process for Managing Change**. Because a border control system must be able to read documents and cards issued by a wide range of authorities (i.e. U.S. federal and state and foreign governments), there must be a forum, outside of the procurement process, for the authorities to discuss the process for deployment, lessons learned, and changing attributes of technology that need to be incorporated by system participants. A forum of this sort needs to be recognized by the agencies involved in the M-1 Committee.

From the perspective of a commercial investor the opportunity to support identity document verification at borders is a good one when judged by criteria 1 through 4 (i.e. volume, time, money and authority). However, this becomes a questionable opportunity when judged by criteria 5 through 7(i.e. standardized technology, existing infrastructure, and process for managing change). This is so because without the forum suggested in 7, there is no place to continue and expand the work of the M-1, and thus no guarantee that the technology will be standardized or that the existing and developing commercial infrastructure will be used.

At this point it is helpful to remember that problems of this sort have been solved in the past by the banking industry and more recently by the Federal government for the distribution of welfare debit cards (i.e. EBT) and the Defense Department’s Common Access Card.

Lessons from Related Efforts Involving Commercial Technology

In the early 1970s the emerging market for credit cards struggled with the problem of interoperability. At the time, each credit card issuer had a unique, proprietary card system. As a result credit cards were not widely accepted. As card use slowly grew, hotels and restaurants were faced with the expense of accepting multiple, unique card systems or turning away customers. The solution for bank issued cards was to create the card association brands we know today as VISA and MasterCard. The card associations, comprised of banks that issued cards and banks that accepted card transactions on behalf of merchants, created committees of their members to preside over technical standards, operating rules for transaction processing and technology upgrades. With the advent of card association brands and consumer protection laws limiting liability, credit card use skyrocketed and equipment costs plummeted.

In the mid 1990s the federal government was faced with a similar problem: how to get all U.S food retailers to accept a standardized debit card, with embedded counterfeit foils, in lieu of food stamps from 26 million Americans. The solution was taken from the card associations. The federal government created a public/private partnership for electronic benefits transfer (i.e. EBT), known as the EBT council. The council adopted the “Quest” brand and functioned very similarly to VISA and MasterCard to standardize card issuance and acceptance. By the late 1990s the Quest brand was accepted throughout the U.S. This also led to the widespread acceptance of consumer debit as well.

In late 1998 the OMB, General Services Administration and the Department of Defense (DoD) collaborated to found the SmartID program, based on the VISA global platform for smart cards and related technology standards. Today, the DoD is in the process of refining its version of the SmartID to incorporate biometrics for logical and physical access. The DoD badge, known as the Common Access Card (CAC) is in the process of being rolled out to all uniformed and civilian military personnel. As such, it is an ideal platform for homeland security badges in the transportation vertical markets.

Elements of the biometric enabled CAC can also be easily adopted to make identity verified travel documents.

Appendix D

California Privacy Related Laws

Appendices D and E are re-compiled by Daniel Greenwood from legislative and other public records

- California Constitution, Article 1, Section 1 The state constitution gives each citizen an "inalienable right" to pursue and obtain "privacy."

- Credit Card Number Truncation - California Civil Code Section 1747.9 No more than the last five digits of a credit card number may be printed on electronic receipts. Effective 1/1/01 for machines put in use on or after that date. Effective 1/1/04 for all machines that electronically print credit card receipts.

- Confidentiality of Medical Information Act - California Civil Code Sections 56-56.37 This law puts limits on the disclosure of patients' medical information by medical providers and health plans.

www.leginfo.ca.gov/cgi-bin/calawquery?codesection=civ&codebody=&hits=20

- Confidentiality of Social Security Numbers - California Civil Code Section 1798.85 This law restricts businesses from publicly posting or displaying Social Security numbers. The law takes effect gradually from 7/1/02 through 7/1/05.

- Consumer Credit Reporting Agencies Act - California Civil Code Section 1785.1-1785.35 This law, the state counterpart of the Fair Credit Reporting Act, regulates consumer credit reporting agencies. It requires them, among other things, 1) to provide free copies of credit reports to consumers who have been denied credit or who are identity theft victims, 2) to block information that appears on a report as the result of identity theft, 3) to place security alerts (effective 7/1/02) or freezes (effective 1/1/03) on the files of consumers who request them, and 4) to provide, for a reasonable fee, credit score information to consumers who request it.

- Destruction of Customer Records - California Civil Code Sections 1798.80 - 1798.82 This requires businesses to shred, erase or otherwise modify the personal information in records under their control.

- Identity Theft: Access to Financial Records on Fraudulent Accounts - California Civil Code Section 1748.95, California Financial Code Sections 4002 and 22470. Similar to Penal Code section 530.8, these laws require certain types of financial institutions to release (to a victim with a police report or to the victim's law enforcement representative) information and evidence related to identity theft.

□Identity Theft - California Penal Code Sections 530.5-530.8
These code sections define the specific crime of identity theft, require the law enforcement agency in the victim's area to take a police report, allow a victim to get an expedited judicial ruling of factual innocence, require the Department of Justice to establish a database of identity theft victims accessible by law enforcement and victims, and require financial institutions to release information and evidence related to identity theft to a victim with a police report or to the victim's law enforcement representative.

□Identity Theft Victim's Rights Against Claimants - Civil Code Section 1798.92-1798.97 This law protects identity theft victims who are being pursued for collection of debts which have been created by identity thieves. The law gives identity theft victims the right to bring an action against a claimant who is seeking payment on a debt NOT owed by the identity theft victim. The identity theft victim may seek an injunction against the claimant, plus actual damages, costs, a civil penalty, and other relief.

□Information Practices Act of 1977- California Civil Code Sections 1798 and following This law applies to state government. It expands upon the constitutional guarantee of privacy by providing limits on the collection, management and dissemination of personal information by state agencies.

□Investigative Consumer Reporting Agencies Act, California Civil Code Sections 1786-1786.56 This law regulates the activities of agencies that collect information on consumers for employers, insurance companies and landlords.

□Legal and Civil Rights of Persons Involuntarily Detained - Welfare & Institutions Code Section 5328 This law provides for the confidentiality of the records of people who are voluntarily or involuntarily detained for psychiatric evaluation or treatment.

□Mandated Blood Testing and Confidentiality to Protect Public Health - California Health & Safety Code Sections 120975-121020

This law protects the privacy of individuals who are the subject of blood testing for antibodies to the probable causative agent of acquired immune deficiency syndrome (AIDS).

□Office of Privacy Protection - California Business and Professions Code Section 350-352 A state law enacted in 2000 created the Office of Privacy Protection, with the mission of protecting and promoting the privacy rights of California consumers.

http://www.leginfo.ca.gov/cgi-bin/displaycode?section=bpc&group=00001-01000&file=350-352

□Patient Access to Medical Records - California Health & Safety Code Section 123110 et seq.

With minor limitations, this law gives patients the right to see and copy information maintained by health care providers relating to the patients' health conditions. The law also gives patients the right to submit amendments to their records, if the patients believe that the records are inaccurate or incomplete.>

□Personal Information Collected on Internet - California Government Code Section 11015.5 This law applies to state government agencies. When collecting personal information electronically, agencies must provide certain notices. Before sharing an individual's information with third parties, agencies must obtain the individual's written consent.

□Public Records Act - California Government Codes Sections 6250-6268 This law applies to state and local government. It gives members of the public a right to obtain certain described kinds of documents that are not protected from disclosure by the Constitution and other laws. It also requires that state and local agencies be "mindful" of the laws that confer privacy rights. This law also provides some specific privacy protections.

□Spam laws - California Business and Professions Code, Section 17538.4 and 17538.45 - Penal Code Section 502 These code section establish the guidelines relating to unsolicited e-mail and faxes.

2002 Privacy Legislation Signed by Governor Davis

Unless otherwise noted, all laws go into effect January 1, 2003.

Identity Theft

AB 1068 (Wright) - Consumer Related Investigations and Credit Reporting: Makes minor changes in the Consumer Credit Reporting Agencies Act and Investigative Consumer Reporting Agencies Act to facilitate implementation by businesses, without weakening the consumer protections added last year by the author's AB 655. Provisions include (1) requiring users of credit reports to take reasonable steps to verify an credit applicant's address if addresses on credit application and credit report vary, replacing former requirement for specific corrective actions; (2) requiring requesters of investigative reports to notify subject in advance and provide form with check box for subject to request copy; and (3) requiring investigative reports to contain notice that information in report may have derived from identity theft and accuracy is not guaranteed. Amends Social Security Number Confidentiality law to grant financial institutions a delay, until 7/1/03, of requirement that SSNs not be printed on statements and similar documents sent through the mail. [Chapter 1030 of 2002] This is an urgency measure, which takes effect immediately.

AB 1155 (Dutra) - DMV documents in ID theft: authorizes courts to impose fines of up to $25,000 on individuals convicted of felony conspiracy to commit ID theft. This bill also makes it a misdemeanor for any person, without

authorization, to obtain (or assist another person in obtaining) a driver's license, identification card, vehicle registration certificate, or other official document issued by the Department of Motor Vehicles. [Chapter 907 of 2002]

AB 1219 (Simitian) - Criminal identity theft: assists victims of criminal ID theft in rectifying criminal records wrongfully associated with their name, by allowing a court or a prosecuting attorney to move for an expedited judicial determination of factual innocence. This bill also allows the court to order the removal of incorrect references to the victim's name and personal information in court records and files. [Chapter 851 of 2002]

AB 1773 (Wayne) - Consolidation of ID theft cases: provides that the jurisdiction for a criminal action for ID theft offenses may be the county where the theft occurred or where the information was illegally used. If multiple ID theft offenses occur in multiple jurisdictions, any one of those jurisdictions is a proper jurisdiction for all of the offenses. Identity theft crimes can occur simultaneously in dozens of counties within the state. Allowing these crimes to be joined and prosecuted in a single county will greatly enhance the prosecution of these crimes. [Chapter 908 of 2002]

AB 2456 (Jackson) - Employment of offenders: provides further limitations on access, by specified prison and county jail inmates, to personal information. Also applies same prohibitions to offenders performing community service in lieu of a fine or custody.

AB 2550 (Nation) - Electronic death registration system: requires the implementation of an electronic death registration system by January 1, 2005. This bill is intended to improve the timeliness and efficiency of California's death registration process, thereby expediting the State's ability to curtail the fraudulent use of both the birth and the death record through the timely application of the birth/death cross-matching. [Chapter 857 of 2002]

AB 2868 (Wright) - Consumer Related Investigations and Credit Reporting: Makes minor changes in Consumer Credit Reporting Agencies Act and Investigative Consumer Reporting Agencies Act to facilitate implementation by businesses, without weakening the consumer protections added last year by the author's AB 655. Provisions include, (1) exempting certain resellers of credit report information from some identity theft blocking requirements; (2) requiring investigative consumer reporting agencies to keep copies of reports available for two years rather than three; and (3) adding costs and attorney fees to damages for violations of some technical requirements of the Consumer Investigative Reporting Agencies Act, but removing such violations from eligibility for punitive damages. [Chapter 1029 of 2002] This is an urgency measure, which takes effect immediately.

SB 1239 (Figueroa) - Expansion of identity theft victims' rights: requires consumer credit reporting agencies to provide a victim of ID theft the right to block fraudulent information and to receive a free copy of his or her credit

report once a month for up to 12 consecutive months. [Chapter 860 of 2002] These provisions will take effect July 1, 2003.

SB 1254 (Alpert) - ID theft: expands definition of "personal information" in crime of ID theft to include financial account #s, taxpayer ID, etc. Makes possessing personal information of another with intent to defraud an offense publishable by up to $1,000 and one year in county jail. Also clarifies that Penal Code 530.8, requiring credit issuers to provide ID theft victims with documents related to fraudulent accounts, applies to cell phone companies. [Chapter 254 of 2002]

SB 1259 (Ackerman) - Payment card theft: provides that the knowing and willful possession or use, with the intent to defraud, of a device designed to scan or re-encode information from or to the magnetic strip of a payment card would be punishable as a misdemeanor. This bill also provides for destruction of those devices owned by the defendant and possessed or used in violation, and allows for the seizure of various other computer equipment used to store illegally obtained data. [Chapter 861 of 2002]

SB 1386 (Peace) - Personal information protection in security breaches: requires a business or a State agency that maintains computerized data that includes personal information, as defined, to disclose any breach of the security of that data to any California resident whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person. This bill gives consumers notice that unauthorized individuals have acquired their personal and/or financial information, thereby giving them the opportunity to take proactive steps to ensure that they do not become victims of identity theft. [Chapter 915 of 2002] These provisions will take effect July 1, 2003.

SB 1617 (Karnette) - Substitute credit cards: requires a credit card issuer that issues a substitute credit card to provide an activation process where consumers are required to contact the card issuer to activate the credit card before it can be used. [Chapter 862 of 2002]

SB 1730 (Bowen) - Credit reporting agencies and Social Security numbers: makes technical changes in last year's SB 168, including an exemption from security freezes for credit monitoring services and others who request credit reports to provide them to consumers, and an exemption, from the requirement to place a security alert or freeze on a credit report, for fraud prevention services. Also amends the SSN confidentiality law (1) to provide that employers administering employee health plans are subject to the same compliance timeline as health plans, and (2) to allow the mailing to consumers of documents containing SSNs when they are part of a process of (a) application or enrollment, (b) establishing or amending an account, or (c) confirmation of the accuracy of the SSN. [Chapter 786 of 2002]

SB 1765 (Bowen) - Warranty cards: requires product warranty cards to clearly state that the consumer is not required to return the card for the warranty to take effect. [Chapter 306 of 2002]

Control of Personal Information

AB 2191 (Migden) - Medical records confidentiality: adds pharmaceutical companies to the list of health care providers, health insurance carriers and contractors that are prohibited form disclosing a patient's medical information without first obtaining authorization. The bill also prohibits a pharmaceutical company from requiring a patient to authorize disclosure in order to receive medications. [Chapter 853 of 2002]

SB 247 (Speier) - Access to birth certificates: reduces the fraudulent use of birth certificates in identity theft by establishing authorization requirements for applicants to obtain certified copies of birth and death certificates. It further requires State and local registrars that issue copies of birth certificates to non-authorized applicants to print the words "informational, not a valid document to establish identity" on the copy issued. [Chapter 914 of 2002]

SB 1614 (Speier) - Public disclosure of birth/death indices: safeguards individual privacy and prevents fraud while allowing necessary public access to birth and death records. This bill exempts specified birth and death indices from disclosure under the California Public Records Act and requires the State Registrar to establish separate non-comprehensive indices, which do not contain Social Security numbers or mother's maiden name, for public release. Requesters of the indices would be required to provide proof of identity and sign a standard form certifying, under penalty of perjury, that they will comply with prescribed guidelines for use of the indices. [Chapter 712 of 2002]

Unwanted Calls, Mail, Email, Faxes

AB 1769 (Leslie) - Unsolicited text ads: prohibits unsolicited text ad messages on cell phones and pagers. [Chapter 699 of 2002]

SB 1560 (Figueroa) - State do-not-call list: amends last year's SB 771, creating the do-not-call list in the AG's Office. Allows small businesses to pay reduced rates for purchasing the list and sets start date for the list as April 1, 2003 (rather than the January). [Chapter 698 of 2002]

AB 2944 (Kehoe and Bowen) - Unsolicited fax ads: repeals California's ineffective junk fax law, allowing California to enforce the federal Telephone Consumer Protection Act's provisions banning unwanted ads sent over fax machines. [Chapter 700 of 2002]

Appendix E

Fair Information Practice Principles

These widely accepted Fair Information Practice Principles are the basis for many privacy laws in the United States, Canada, Europe and other parts of the world. The principles were first formulated by the U. S. Department of Health, Education and Welfare in 1973, and are quoted here from the Organisation for Economic Cooperation and Development's Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (available at http://www1.oecd.org/publications/e-book/9302011E.PDF).

Openness

There should be a general policy of openness about developments, practices and policies with respect to personal data. Means should be readily available for establishing the existence and nature of personal data, and the main purposes of their use, as well as the identity and usual residence of the data controller.

Collection Limitation

There should be limits to the collection of personal data and any such data should be obtain by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject.

Purpose Specification

The purpose for which personal data are collected should be specified not later than at the time of data collection and the subsequent use limited to the fulfillment of those purposes or such others as are not incompatible with those purposes and as are specified on each occasion of change of purpose.

Use Limitation

Personal data should not be disclosed, made available or otherwise used for purposes other than those specified as described above, except with the consent of the data subject or by the authority of law.

Data Quality

Personal data should be relevant to the purposes for which they are to be used, and, to the extent necessary for those purposes, should be accurate, complete, relevant and kept up-to-date.

Individual Participation

An individual should have the right: a) to obtain from a data controller, or otherwise, confirmation of whether or not the data controller has data relating to him; b) to have communicated to him, data relating to him within a reasonable time; at a charge, if any, that is not excessive; in a reasonable manner; and in a form that is readily intelligible to him; c) to be given reasons if a request is denied and to be able to challenge such denial; and d) to challenge data relating to him and, if the challenge is successful, to have the data erased, rectified, completed or amended.

Security Safeguards

Personal data should be protected by reasonable security safeguards against such risks as loss or unauthorized access, destruction, use, modification or disclosure of data.

Accountability

A data controller should be accountable for complying with measures, which give effect to the principles stated above.

Appendix F

Public/Private Consortium Identity System[8]

By Helena Sims

Purpose

Another alternative approach to the problem of identity management is the development of a public/private partnership that would create commercially-based operating rules to achieve interoperability between identity verification systems for workers across the aviation, highway transport and maritime sectors.

Background

Interoperability is fundamental to the efficient and cost-effective operation of identity verification systems. The need for interoperability is becoming more apparent with congressional enactment of legislation calling for the verification of individuals at a broad array of security-sensitive, access control points. For instance, the Aviation and Transportation Act requires the identity verification of airline and airport workers. The U.S. Patriot Act addresses identity verification for hazardous materials truck drivers. Other legislation addresses maritime workers, and security at border crossings. To promote seamless communication between these systems, and to avoid the duplication of hardware and other resources, it is important to promote system interoperability.

Recent experience has demonstrated that system interoperability can be achieved through a commercial rules-based process. For instance, payment networks, such as VISA and PLUS, rely on operating rules to achieve nationwide interoperability between participants. In addition, individual states' electronic benefits transfer (EBT) systems are interoperable because states have opted to use a common set of commercially based operating rules, known as the Quest Operating Rules. These rules are developed and maintained by a public/private partnership. They spell out the rights, responsibilities and liabilities of those participating in the Quest network.

Similarly, interoperability could be achieved between identity verification systems if a common set of commercially based operating rules were developed by government and industry stakeholders.

Commercially-based operating rules have a number of advantages when compared to government regulations. Because they are collaboratively developed by government and private sector stakeholders, participants tend to develop a sense of ownership towards the rules. The rules are made enforceable through a series of contracts between participants and are therefore

[8] A Uniform Identity Verification and Access System

enforceable in court, rather than being subject to regulatory enforcement. In addition, the rules can be amended in a timely manner, which is important in an industry that is likely to adopt new procedures and technologies over time.

Government sovereignty is not compromised in a commercially based rule-making process, because operating rules must be consistent with state and federal laws and regulations. For instance, the Quest Operating Rules are consistent with government regulations and are adopted at the discretion of each state. States have veto authority over the rules and any amendments to them.

Finally, in proposing commercially based rules for identity verification systems, it is assumed that an identity card will be issued as part of the process.

The Key to Interoperable Systems: Operating Rules

Using a consensus-based process, an independent, non-profit organization could develop operating rules to govern the rights and responsibilities of those that participate in identity verification systems, and specify the standards for identity cards and card readers used throughout the system. These Identity Verification and Access Security rules, referred to here as IVAS rules, could form the foundation for a national homeland security brand, much as credit and debit card companies have branded VISA, MasterCard and PLUS. Elements covered by the IVAS rules would include:

- An identity proofing and enrollment process to register individuals based on common credentials.
- Criminal and economic history background checking and adjudication.
- Agreements required between participants.
- Certification requirements for issuers and access transaction acquirers.
- Identity card standards.
- Containers on cards that must be used for interoperable applications.
- Containers on cards that may be used for local applications.
- Biometrics requirements.
- System security features.
- Identity card security features.
- Identity card issuance.
- Identity card acceptance.
- Database and system maintenance requirements.
- Required ANSI, ISO, ICAO and AAMVA standards.
- Rights, responsibilities, warranties and liabilities of the participants.
- Enforcement (arbitration, fines and other remedies).
- Phase-in periods for some provisions.

Some of the elements listed above could be performed by governments, some could be performed by entities under contract to governments, and some could be conducted by private sector entities bound to other participants by contract.

Rule-Making Body

A broad cross section of private and public sector stakeholders could work cooperatively to develop operating rules. Involving stakeholders in the development process ensures that various points of view are considered. Possible participants in the organizational, operational and maintenance phases include, but are not limited to, representatives from:

Government Entities

- Federal Agencies
  - Department of Commerce
  - Department of Defense, National Security Agency
  - Department of Justice
  - Department of Transportation
    - Federal Aviation Administration
    - Federal Motor Carrier Safety Administration
    - Federal Railway Administration
    - Federal Transit Administration
    - Maritime Administration
    - Transportation Security Administration
- Environmental Protection Agency
  - General Services Administration
  - Office of Homeland Security
- State and Local Governments
- Law Enforcement Agencies

Quasi-Government Agencies

- Airports
- Ports
- Utilities

Private-Sector Organizations

- Trade associations
- Airlines
- Shipping companies
- HAZMAT production and disposal facilities
- Trucking companies
- Employee organizations and unions
- Vendors
- Insurers
- Systems integrators

Advantages to Common Operating Rules

- Nationwide interoperability of identity verification and access systems.
- No need to reissue and re-adjudicate IDs when employees change jobs.
- Cost savings driven by:
  - A large volume purchase made possible by appropriated funds;
  - Implementation on a date certain.
- Standardized technology; and
  - An open platform that promotes bids by multiple vendors.
- Inclusive process for managing change in technology, attitudes, infrastructure, etc.
- Governments could rely upon, not duplicate, commercial infrastructure.

Appendix G

e-Authentication Risk and Requirements Analysis (e-RA) Process

Contributed by William Wilson

The Software Engineering Institute (SEI) at Carnegie Mellon University has developed a risk-based process for identifying authentication requirements for operational systems called e-RA, or e-Authentication Risk and Requirements Analysis. The broad objectives of the e-RA process are to:

- Document and characterize a system's transactions and associated data.
- Identify the risks associated with authentication of the actors (or users) for the system's range of transactions.
- Define the authentication requirements for the system's transactions within a prescribed set of authentication criteria.

The e-RA process is performed in three primary activities: data collection, risk analysis, and requirements definition. Throughout these activities, there are two types of workshops performed – interview-style workshops with system developers and users, and analysis-style workshops for performing analysis on the collected information and producing the final set of outputs. Each of these primary activities is briefly described below.

Data Collection. Data collection activities are focused on identifying and characterizing the system's transactions. This is accomplished through a facilitated workshop in which participants from the systems development and user communities identify the critical and common transactions that form the basic user functionality of the system. Detailed information about these transactions is gathered including the types of users who might use the transactions, where the transactions can be initiated (such as over the public Internet), and the type and nature of data that is associated with the transaction.

Risk[9] Analysis. In the risk analysis workshop, participants begin by building a set of "impact evaluation criteria" which define the system owner's impact areas (such as reputation, legal, and financial) and their risk tolerances (their definitions of high, medium, and low impacts for each area). For each transaction identified in the data collection workshop, participants are then asked to describe the impacts that could result if an *unauthorized user*[10] executed the transaction. This

[9] A risk is considered to be the combination of transaction, the impacts of an unauthorized actor using that transaction, and a measure of the severity of these impacts on the system and its owners.

[10] An unauthorized user is described as one whose use of the transaction would not have been intended. In

threat scenario combined with the resulting impacts defines a risk for the transaction, the system, and its owners. Each of these risks are then measured with the "impact evaluation criteria" to determine the extent to which the various constituents of the system would be affected if the risk is realized.

Requirements Definition. In the final activity, the information gathered in data collection and risk analysis is used to determine the authentication requirements of each transaction. The nature of the transaction, the potential impacts that could occur if unauthorized users use the transaction, and the degree of severity of the impact are analyzed. This analysis results in the identification of authentication requirements for each transaction. These requirements are based on mapping the transactions to user-prescribed authentication criteria. Cumulatively, this defines the authentication requirements of the system.

Four pilots of an initial expert-led version of the e-RA process have been completed. This version gathered information from participants, but the risk analysis and requirements definition activities were performed by SEI staff. Lessons learned in these pilots are being integrated into a revised approach where participants perform an assessment on their own systems in an instructor-led workshop approach. This approach is being developed in a partnership with the GSA Office of E-Government for deployment to the e-government initiatives beginning in November 2002.

---

other words, they would not normally be authorized to perform the action that the transaction enables.